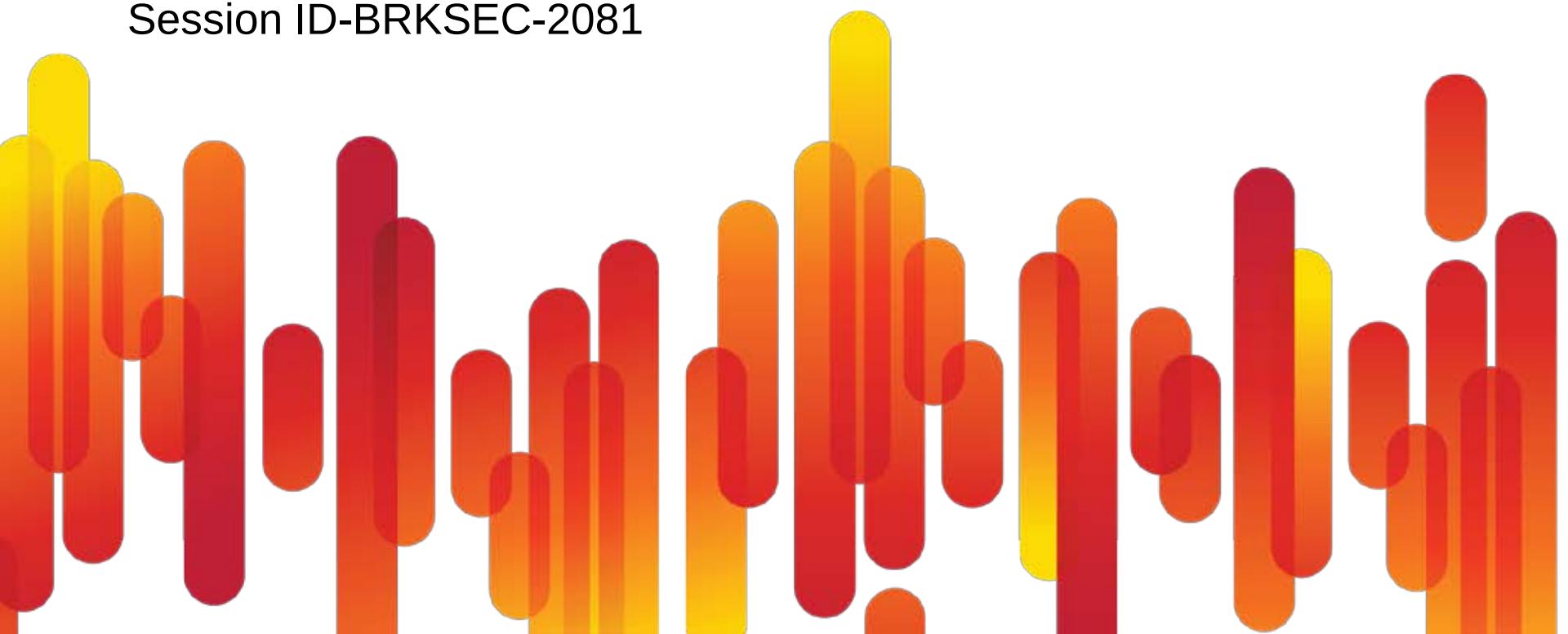
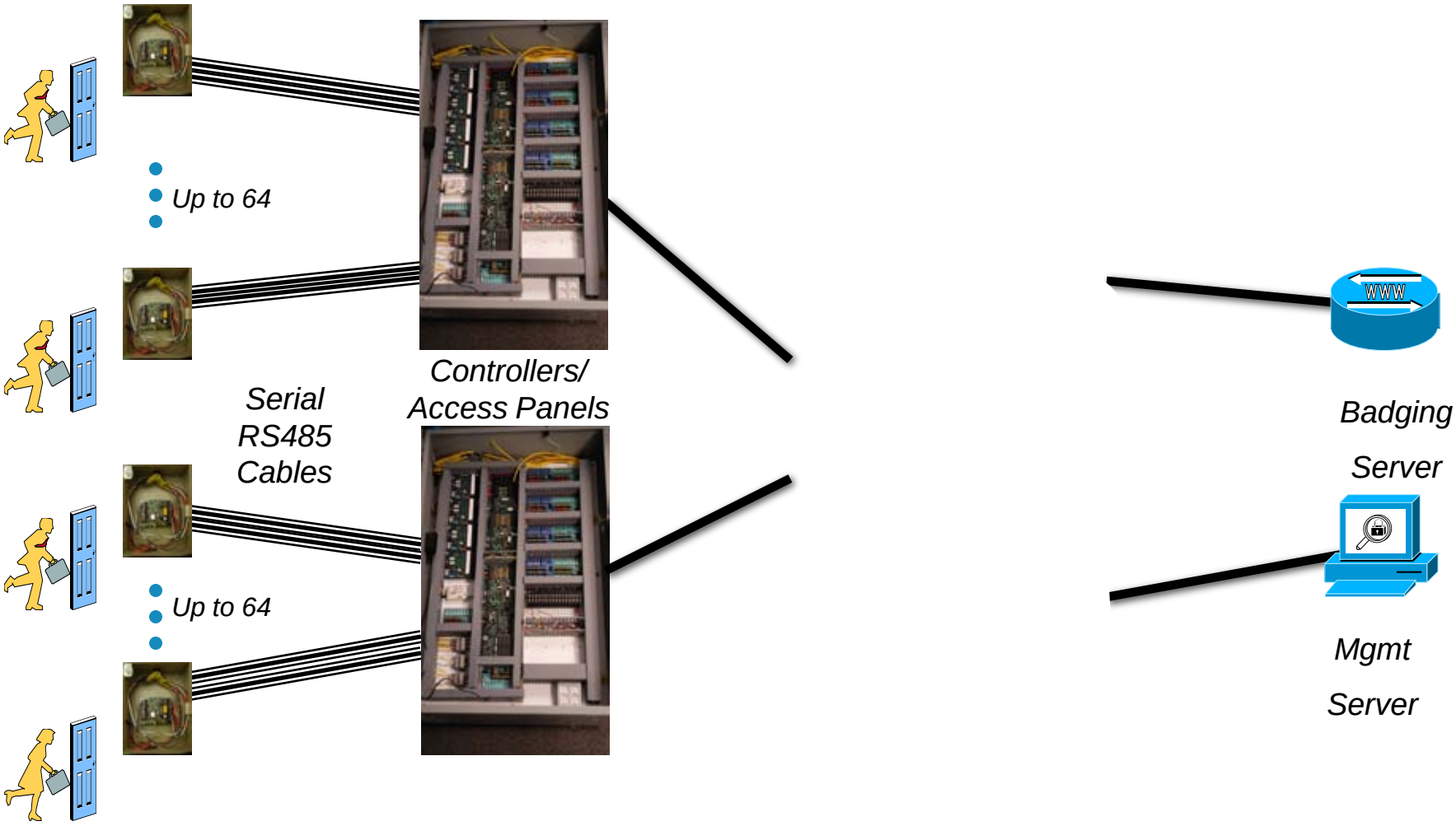
Implementation of Cisco Physical Access Control

Session ID-BRKSEC-2081

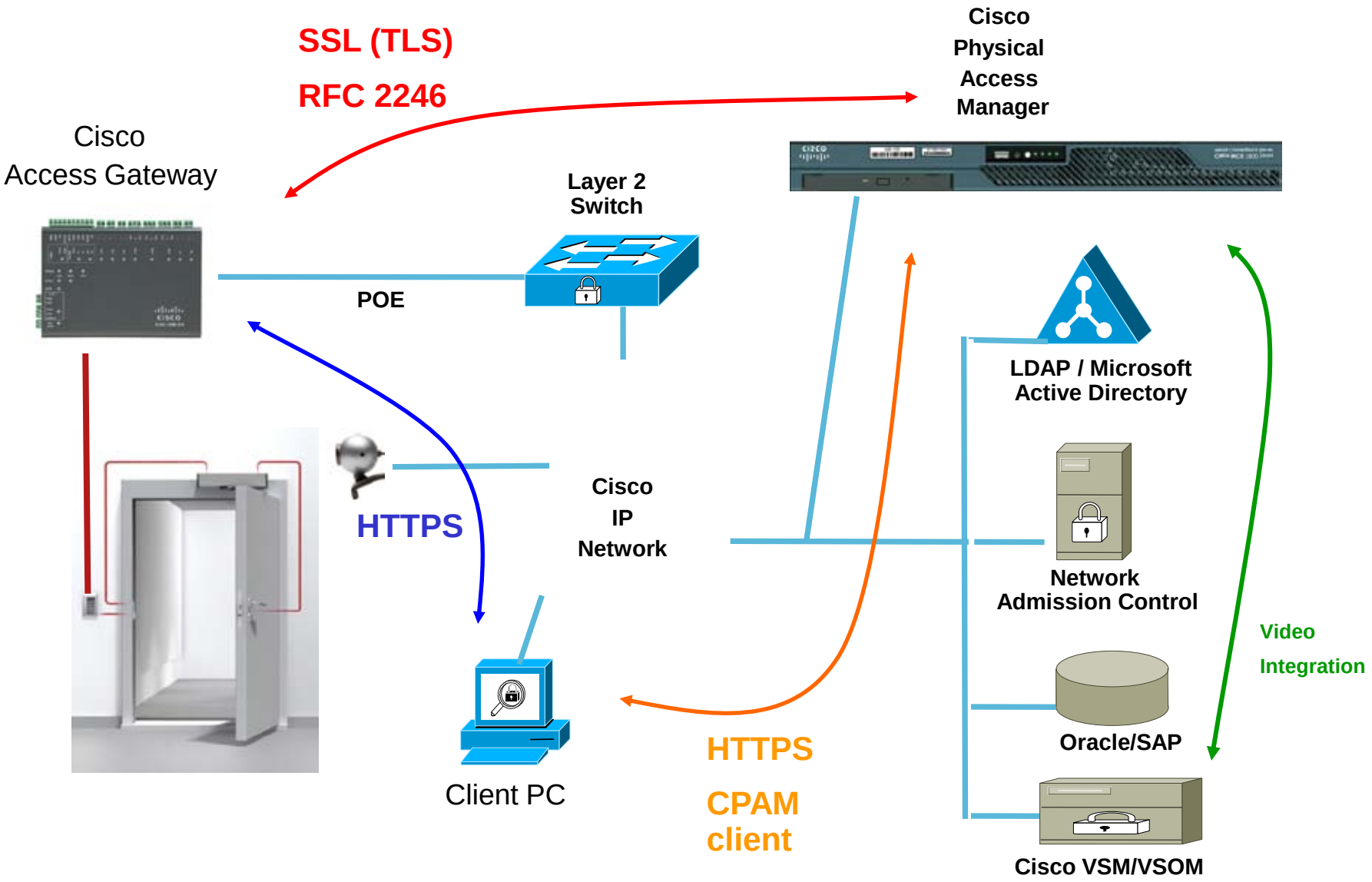


Access Control Architectures of yesteryear



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Access Control Deployment Architecture



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Product Overview

- Hardware:

  Cisco Access Gateway controlling a door

  Additional modules for readers, inputs and outputs can be connected to the Access Gateway via a CAN bus. (more on this later)

- Software:

  Cisco Physical Access Manager (CPAM): A management application with rich interfaces to IT applications and Identity stores.

  Web interface to Gateway for local management and monitoring

  Enterprise Data Studio for IT integration to existing employee data bases

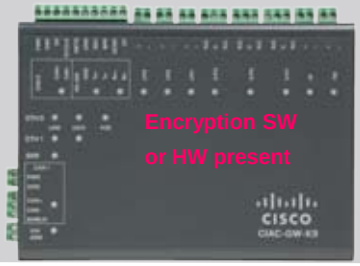
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Access Control Hardware Modules

1. **Access Gateway: CIAC-GW-K9** can manage 1 or 2 doors depending on associated reader and devices. Up to 15 additional modules can be connected. (K9 signifies encryption hardware or software is present)
2. **Reader Module: CIAC-GW-RDR** Controls up to two readers, connects to one Access Gateway via CAN bus
3. **Input Module: CIAC-GW-IP10** Controls 10 inputs, connects to one Access Gateway via CAN bus
4. **Output Module: CIAC-GW-OP8** Controls 8 outputs, connects to one Access Gateway via CAN bus

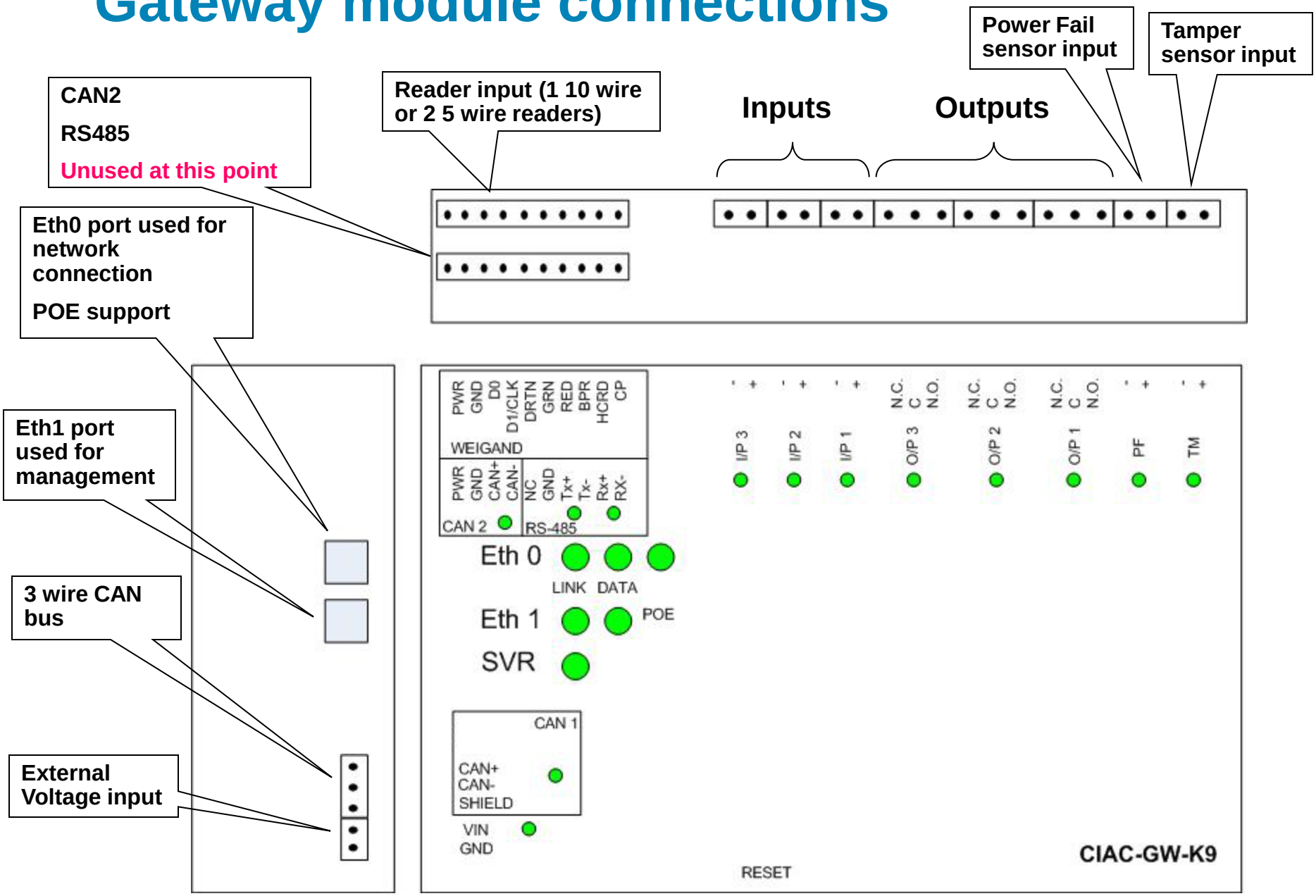
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hardware Module Overview

Cisco Physical Access Gateway	Reader Module	Input Module	Output Module
			
▪ Mandatory component. Connects up to 2 doors, and up to 15 additional modules (connected via a 3 wire CAN bus). ▪ Power: POE or 12V to 24V DC ▪ 2 Ethernet ports ▪ 10 pin Weigand Reader port : can be configured as two 5 pin Weigand ports ▪ 1 RS-485 port ▪ 3 Outputs (Form C Relays) ▪ 3 Supervised inputs ▪ Tamper & PF inputs (can be configured as additional inputs)	▪ Requires Access Gateway ▪ Connects up to 2 doors, to the Cisco Access Gateway via CAN bus. ▪ Power: 12V to 24V DC ▪ 10 pin Weigand port : can be configured as two 5 pin Weigand ports ▪ 1 RS-485 port ▪ 3 Outputs (Form C Relays) ▪ 3 Supervised inputs ▪ Tamper & PF inputs (can be configured to be used as additional inputs) ▪ CAN Termination switch	▪ Requires Access Gateway ▪ Connects up to 10 inputs to the Cisco Access Gateway via a CAN bus. ▪ Example inputs are: Pushbutton switches, Glass Break sensors, or any contact closure input. circuit ▪ Power: 12V to 24V DC ▪ 10 Supervised inputs ▪ Tamper & PF inputs (can be configured to be used as additional inputs) ▪ CAN Termination switch	▪ Requires Access Gateway ▪ Connects up to 8 outputs to the Cisco Access Gateway cia CAN bus.. ▪ Example outputs are: lights, LEDs, or any contact closure output circuit. ▪ Power: 12V to 24V DC ▪ 8 Form C (5A, 30V) outputs ▪ Tamper & PF inputs (can be configured to be used as additional inputs) ▪ CAN Termination switch

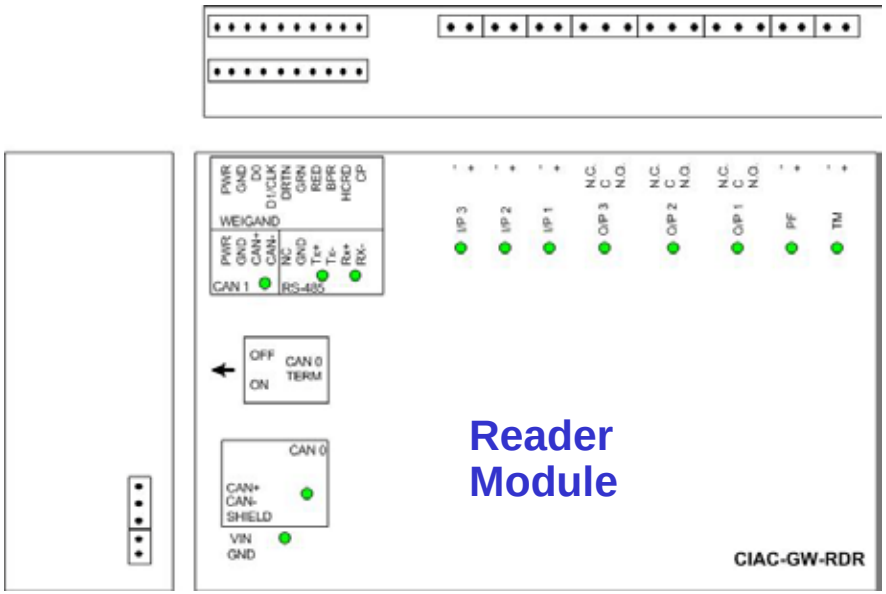
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

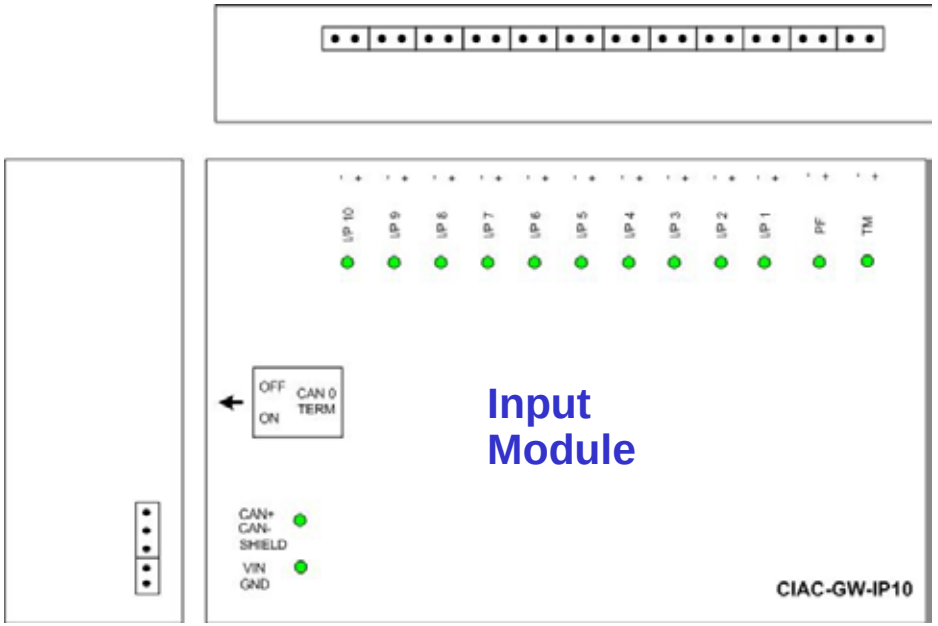
Gateway module connections

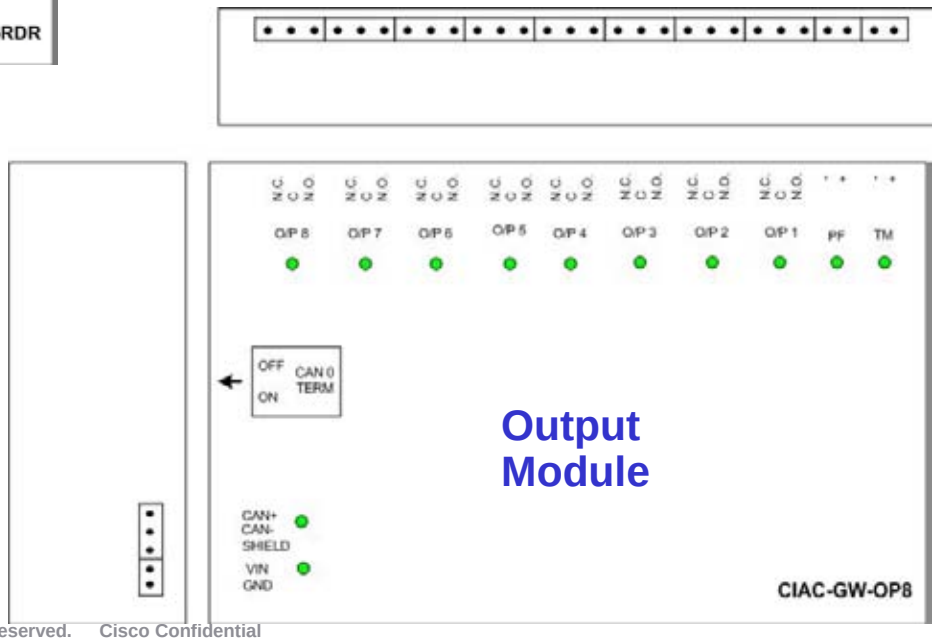


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Additional modules







Require external power to operate

Connected to Gateway module via 3 wire CAN bus. No other network connectivity.

Each of these modules can function as a CAN termination module.

Verify termination switch setting on each module.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Physical Access Manager (CPAM)

- Appliance form factor 1 RU server:
  - WebStart-based client-server architecture
  - Rich role-based access control (RBAC) policies using prifiles
  - Access control policies (two-door, anti-passback, etc.)
  - Ease of configuration and administration
  - Server pair deployment between Cisco Physical Security Manager instances
  - Badge enrollment and design
  - Reporting (template based reports and custom reports)
  - Fully integrated with Cisco VSM server 3.1.1/5.1.1 thru 4.2/6.2
  - Global I/O and Device I/O policy management

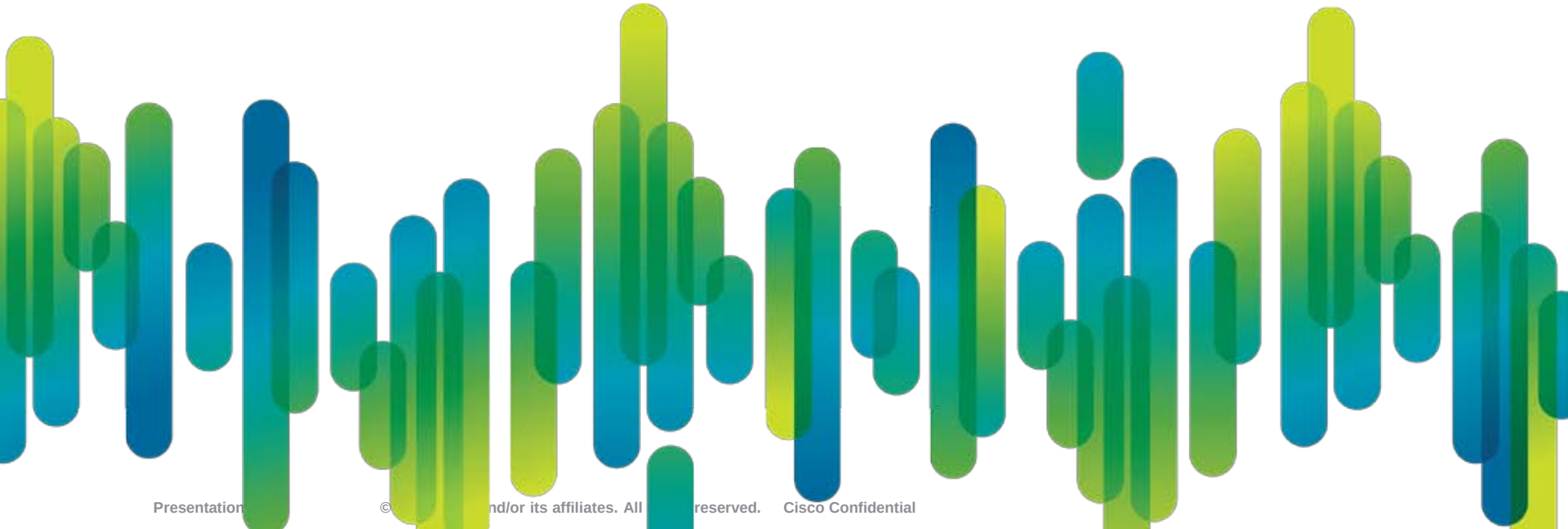
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video Integration

- Video integration with Cisco VSM Suite: Video associated with device (door) can be pulled up instantly
- Video settings done on a per CPAM user profile basis.
- Associate a camera and its PTZ setting with an event/device.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Solution Details



© nd/or its affiliates. All reserved. Cisco Confidential

The CPAM server

- CPAM server is first device to setup and install.
- ISO image is based on RedHat Enterprise Server 4.x
- CPAM application is included on ISO, and upgraded via the normal Linux RPM process. (under the covers)
- Web based access to manage and configure the server once it is installed.
- Client (Micro Soft only at this point) is downloaded from the server, and used to manage, monitor, and configure the rest of the hardware

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The CPAM server (continued)

- Install and IP addressing
- HA considerations
- Upgrade
- Configuration backup and restore
- Licensing

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CPAM server Install

- CPAM server comes pre-loaded from factory
- Also can be installed from scratch using ISO image and CD/DVD.
- Default IP for ETH0 after a fresh install is 192.168.1.2.
- Initial username and password are ***cpamadmin***
- Upon first login to CPAM web server, you are prompted to continue the initial configuration of the server.

Select the server type Active or Standby

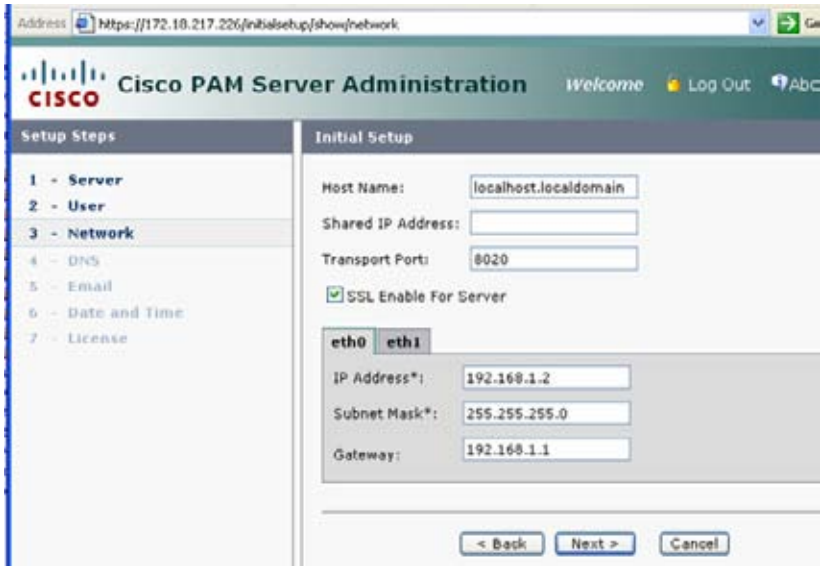
Enter the Site Name….only for Active Server

Don't use space in the site name

Under the User panel you will be prompted to change the password for user cpamadmin. Client will use this password for login until changed. User cpamadmin can have different passwords for web admin and client login there after

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Install continued



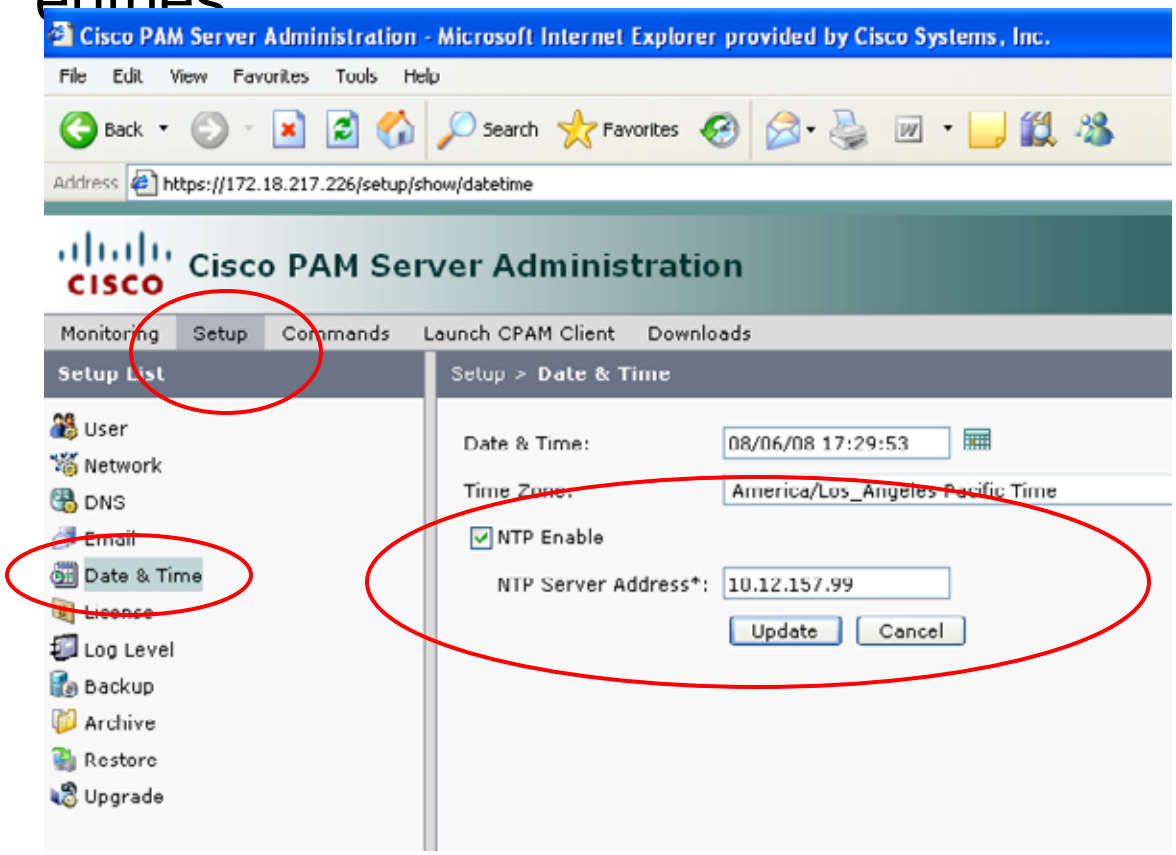
Under the Network panel, you are prompted for the Host name, Eth0 IP, and Shared IP Address if you are configuring for a Standby server operation. You also have the option to enter a non-default TCP port if you wish. The default is 8020. SSL is enabled by default.

- **After configuring the information on this interface, the server application is restarted.**
- **User will then continue with DNS, Email, Date and Time, and License settings.**
- **After licensing information is entered, the application restarts and completes the install.**

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

NTP (Network Timing Protocol)

- Standards method to ensure all devices clocks are in sync resulting in correlated timestamps on log entries



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

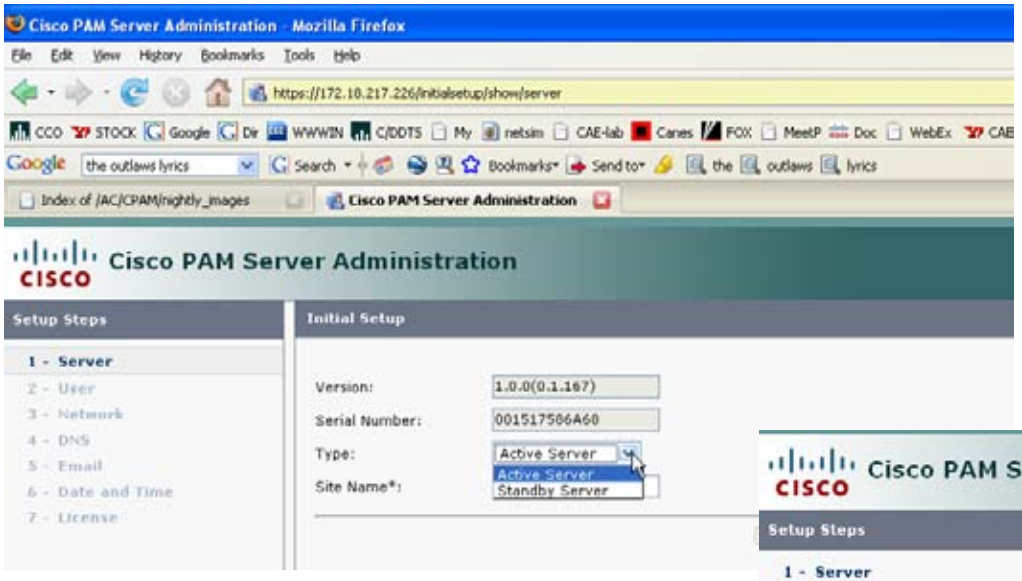
High Availability for CPAM

- Active Server ETH0 IP address
- Standby Server ETH 0 IP address
- Shared IP address
- All must share same subnet
- Active and Standby keep the configuration in sync between them
- Stopping the Active Server via the web interface triggers the standby to go active.
- If active server powers down, or is shutdown, lack of keep alive frames as seen by the standby server triggers it to become active.
- Standby server assumes module licenses from the active server Standby server operation is a licensed feature.
- Switch over is non-disruptive to operation and not automatically reverted if the original active server comes back up.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

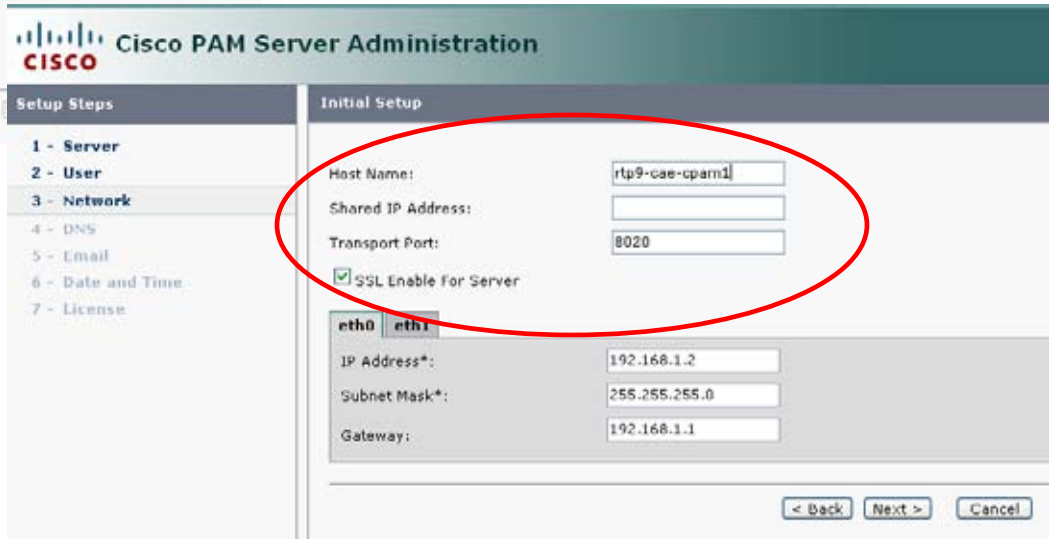
High Availability for the CPAM server

- Type determined at initial install time.



Active server should be brought online prior to the Standby server being brought online.

Active, Standby, and Shared IP address must be on the same IP subnet.



The server pair exposes a single IP address. The active server owns the address in the normal state. Should the active server fail, the standby server assumes ownership of the shared IP address.

Clients and Gateways must reconnect after failover occurs.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco PAM High Availability

Utilizes LINUX-HA project for this. (http://linux-ha.org) for more details.

At install time servers are designated either **Active** or **Standby**.

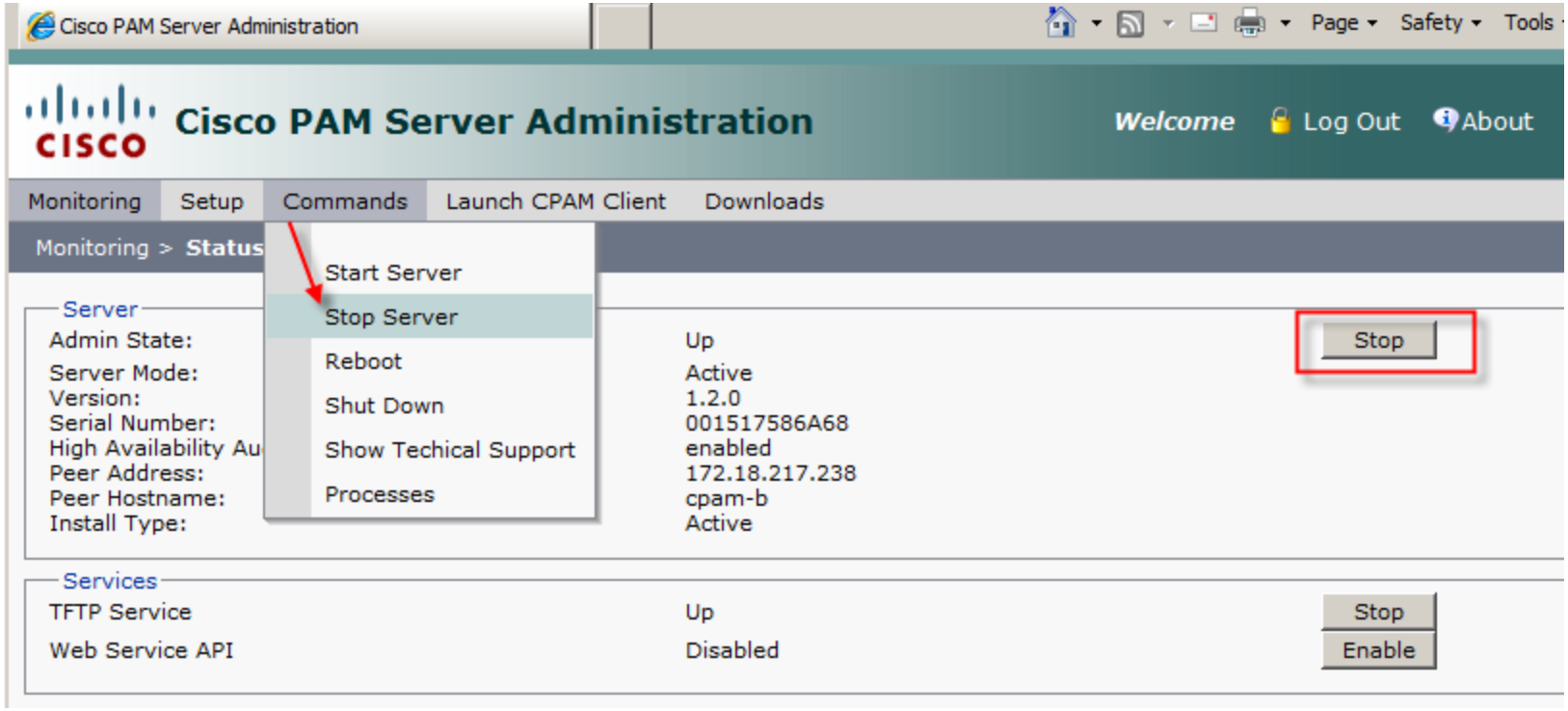
All licenses except the HA license are keyed by serial number, and installed on the Active Server.

The HA license is keyed by serial number, and installed on the Standby Server.

Once HA pair is established, the licenses are copied to the other server, resulting in both servers containing all licenses.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

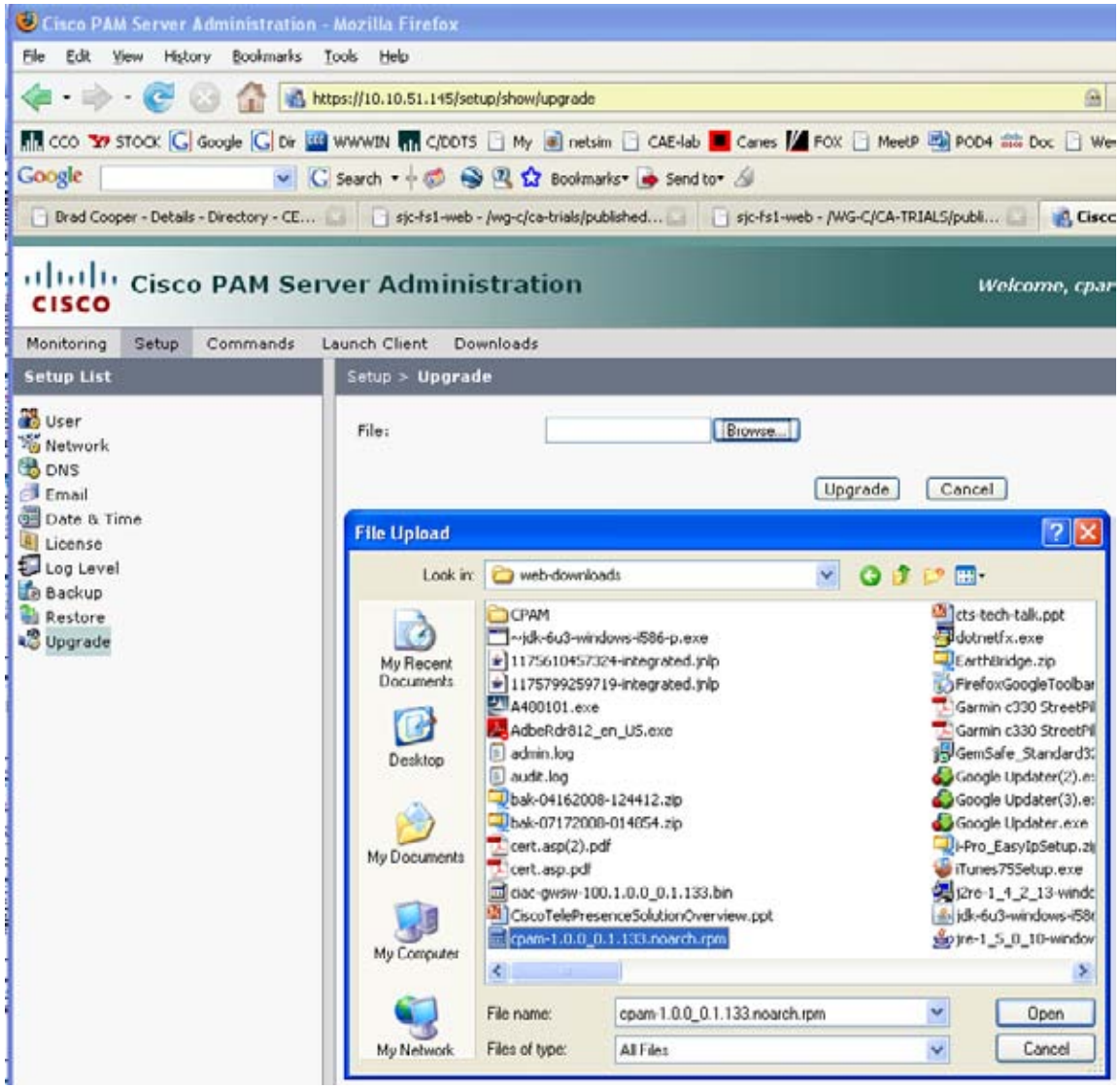
Stopping the CPAM server application



Stop option is available on the Monitor Screen, or under the Commands tab.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Software upgrades for CPAM server, CPAM is always upgraded first, then the Gateway modules



Upgrade option is located under the Setup menu.

Option to browse for a file on the client machine to use for the upgrade.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

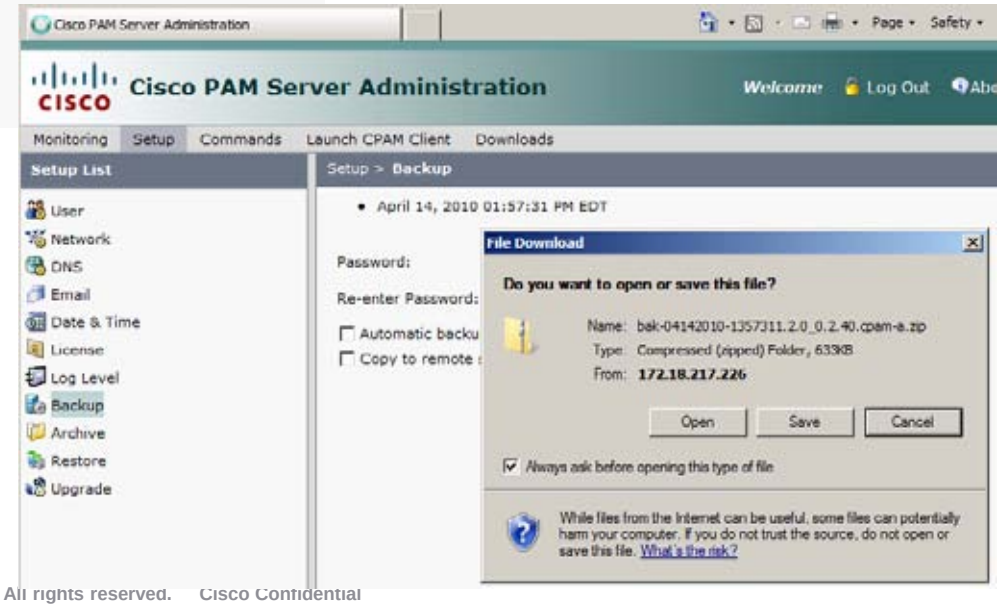
CPAM database backup

Performed from the CPAM web interface

Backup is located under the Setup menu

Once completed on the CPAM server you can download and save the file on the client machine, or network attached drive.

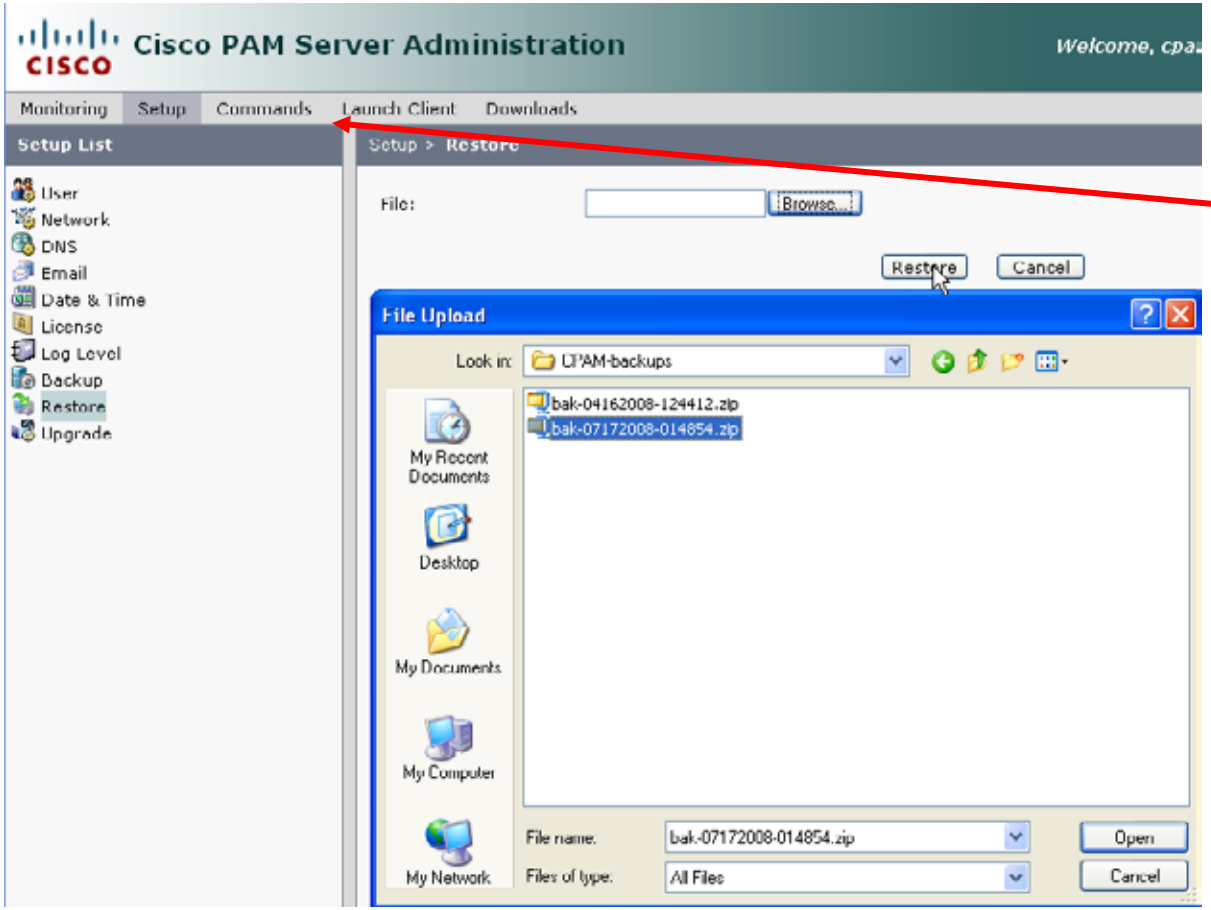
Back up file is encrypted, and requires a password when created.


Cisco PAM Server Administration
Cisco PAM Server Administration
Welcome
Log Out
Monitoring
Setup
Commands
Launch CPAM Client
Downloads
Setup List
Setup > Backup
April 14, 2010 01:57:31 PM EDT
Password:
Re-enter Password:
File Download
Do you want to open or save this file?
Name: bak-04142010-1357311.2.0_0.2.40.cpam-a.zip
Type: Compressed (zipped) Folder, 633KB
From: 172.18.217.226
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Automated backup, and remote file placement are available.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CPAM database restore



CPAM server application must be stopped before the restore option can be used.

Option to STOP server is under the Commands menu or Monitor - Status panel.

Restore is located under the Setup menu.

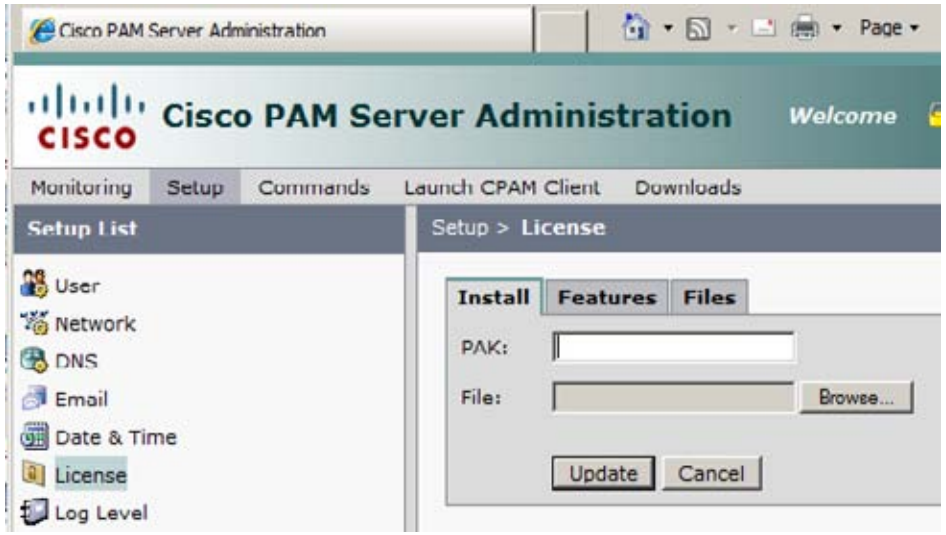
Option to Browse for a backup file located on the client machine or network attached drive..

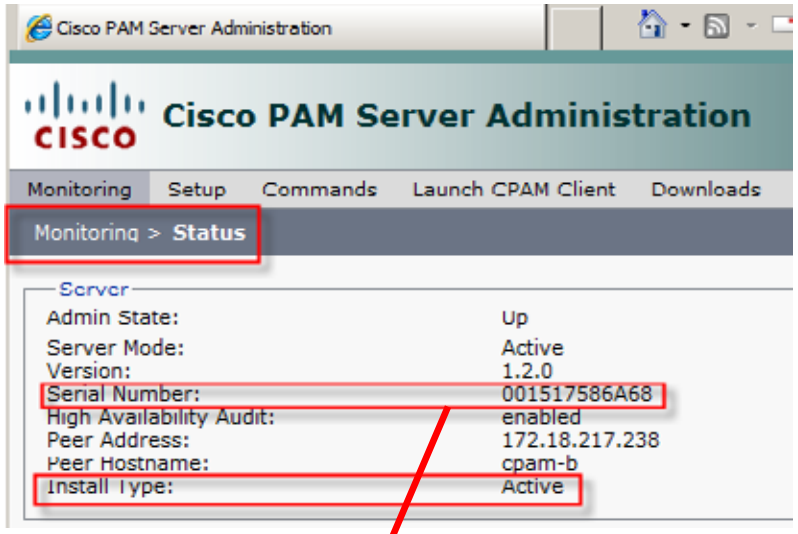
Since file is encrypted, you need to enter the password that was used to generate the file.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Licensing

Installed via WEB connection to CPAM active server.

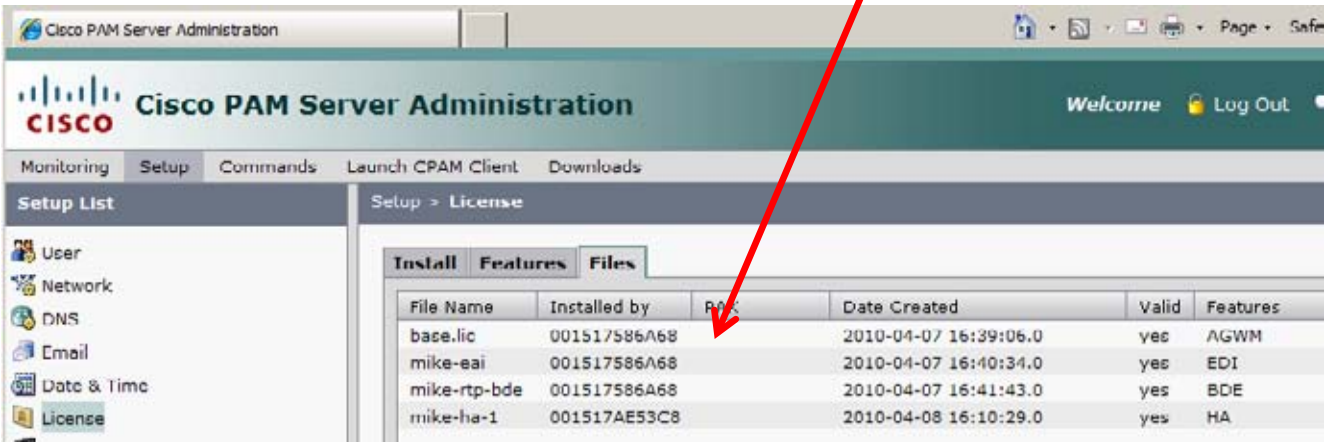




Customer can view installed license files from same menu using the Features or Files tab.

Licensing issues should be directed to licensing@cisco.com.

Licenses are key to server software serial number.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco PAM Licensing Model

Simple licensing model. No limits on number of badges enrolled, or on number of administrative users/ monitors of the system.

Capacity license upgrades for: 64, 128, 512 and 1024 modules (Access GW, Reader, Input or Output), allowing for flexible deployment choices

Module licenses are cumulative.

Additional feature licenses available for the following:

- Badge Designer
- Enterprise Data Integration
- High Availability

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

License SKUs

SKU	Description
CIAC-PAME-BD=	Badge Designer License
CIAS-PAME-HA=	High Availability License
CIAC-PAME-EDI=	Enterprise Data Integration License
CIAC-PAME-WSAPI-	Web Services API License
CIAC-PAME-M64=	Additional 64 modules License
CIAC-PAME-M128=	Additional 128 modules License
CIAC-PAME-M512=	Additional 512 modules License
CIAC-PAME-M1024=	Additional 1024 modules License

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hardware SKUs

SKU	Description
CIAC-PAME-1125-K9	Version 1 CPAM appliance (32 modules licensed)
CPS-MSP-1RU-K9	Version 2 CPAM appliance (32 modules licensed)
CIAS-GW-K9	Gateway Module
CIAC-GW-RDR	Reader Module
CIAC-GW-IP10	Input Module (10 inputs)
CIAC-GW-OP8	Output Module (8 outputs)

Note: CPAM release 1.1 and 1.0 provided support for 4 modules with the bas license installed. If a 1.0, or 1.1 server is upgraded to 1.2, the base license will still support 4 modules. With a fresh install of the 1.2 release, the base license will support 32 modules

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Gateway and associated modules

- Web Configuration Tool.
- Power Over Ethernet
- Initial Configuration
- Configuring the CPAM address and port number
- Additional module information display
- Image management and embedded software
- The CAN bus

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Gateway Module

- The second device to configure and install is the gateway module.
- Powered via POE, or 12 to 24 VDC
- It requires IP address (static or DHCP), the CPAM server IP address, and the TCP port number to use when communicating with the CPAM server.
- Software image is pushed to the gateway module from the CPAM server or directly from the gateway web interface..
- External device attachment to the gateway can be done before, or after the configuration is completed.
- Additional module attachment is made via the 3 wire CAN bus, and are powered via 12 to 24 VDC only. No POE for the add on modules.
- Configuration is loaded to the gateway and the downstream modules via the CAN bus from the gateway module. No user action needed to push configuration to the downstream modules.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

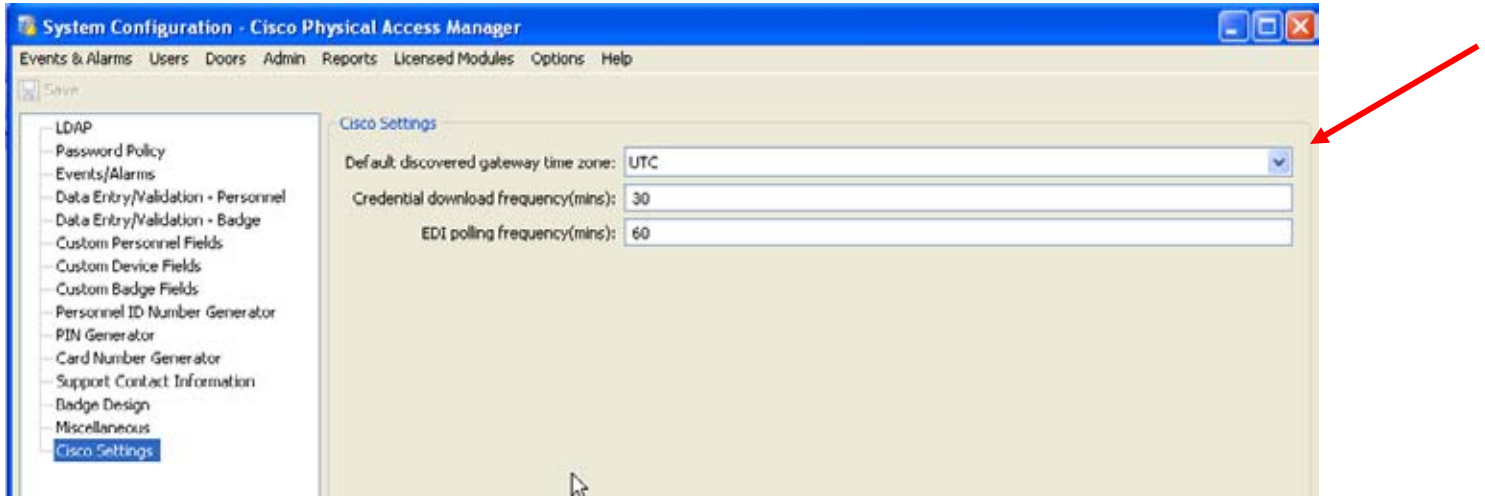
Gateway module Web Configuration tool

- **Eth0** IP Address assignment (connection to IP network)
  - Static (manually assign Gateway module IP, default router, CPAM server IP address, and TCP port number.)
  - DHCP (Which is the module default)
    - DHCP 0ption 150 should be the CPAM server IP address
    - DHCP Option 151 should be the TCP port used
    - Gateway will not fall back to any default IP address if DHCP is configured.
    - Default gateway router, DNS server for the Gateway module and it's IP address are standard DHCP items provided by the DHCP server. You can use a mix of DHCP for these, and static configuration for the CPAM IP and port.
- **Eth1** pre-configured and not alterable
  - Used only for a Mgmt interface
  - IP address set to 192.168.1.42/24

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

NTP

- If NTP is not configured on the gateway , it will use the time from the CPAM server. Under system configuration you can set the default time zone for discovered gateways.
- Gateway time zone should be configured before creating doors on the gateway



If Time on Gateway is + or – 20 seconds from CPAM server, or NTP server, upon connection, the gateway will reload.

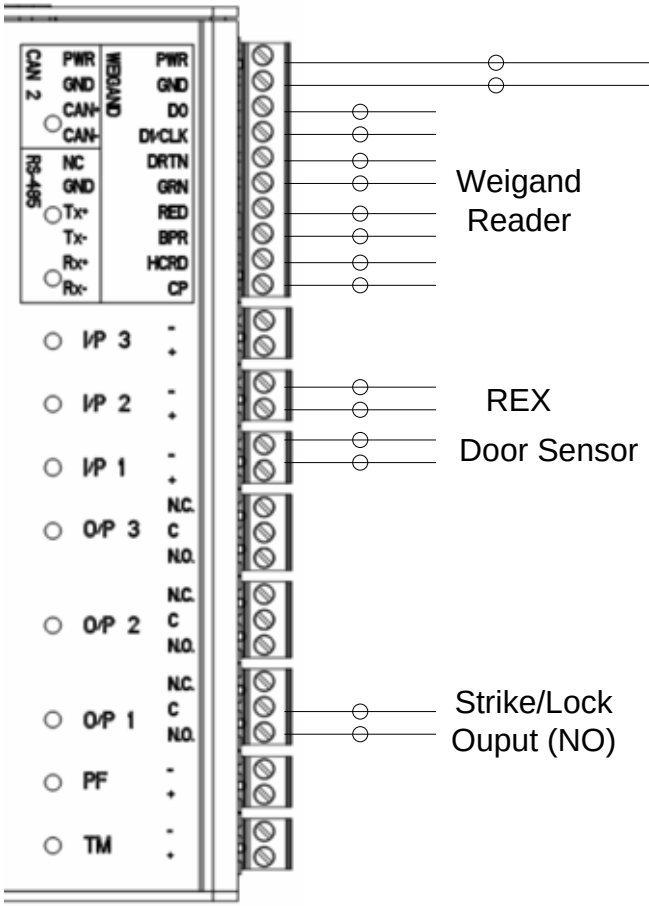
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

POE for the Gateway

- GW POE budget can be used to power readers and locks attached to the Gateway module
- If Aux power and POE are present, Aux power takes precedence. A switch from Aux to POE will cause a gateway reload.
- POE backup should be provided at the POE switch in the datacenter.
- Total external power supplied is limited to 650 mA at 12 V DC (7.8 Watts). This can be used to power readers and a strike, as long as total peak current between all devices is less than 650 mA.
- Wire gauge depends on distance from Gateway: choose 20 AWG for up to 100 Feet.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sample of Single Door POE Connection



Reader & Lock Power: Total Draw 650 mA at 12 V

Weigand Reader

REX

Door Sensor

Strike/Lock Ouput (NO)

Weigand readers can be configured with a single 10 wire interface (including Power and GND) or as two 5 Wire readers. The Power and GND connections are shared between the two readers in this instance.

Example POE Devices		
Device	Description	Peak Current Consumption (mA)
HID 6005	HID Prox Point Reader	75
HES RF5010	HES Integrated Reader & Strike	240

CAN2 and RS-485 connections are for future use.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Weigand slot wiring on Gateway or Reader modules.

	Chassis Label	One 10 Wire	First 5 Wire	Second 5 Wire
10	PWR	PWR (red)	PWR (red)	PWR (red)
9	GND	GND (black)	GND (black)	GND (black)
8	D0	D0 (green)	D0 (green)	----------
7	D1/CLCK	D1/CLCK (white)	D1/CLCK (white)	----------
6	DRTN	DRTN (shield)	DRTN (shield)	DRTN (shield)
5	GRN	GRN (orange)	GRN (orange)	----------
4	RED	RED (brown)	----------	GRN (orange)
3	BPR	BPR (blue)	----------	----------
2	HCRD	HCRD (yellow)	----------	D1/CLCK (white)
1	CP	CP (purple)	----------	D0 (green)

Wire colors show in parentheses

---------- means wire slot is unused

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Initial configuration of the Gateway module using Eth1

Cisco Access Control Gateway - Login - Microsoft Internet Explorer provided by Cisco Systems...
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.42
Go Links
CISCO
Cisco Access Control Gateway
1.0.0
Username
Password
Log In
Cancel
© 2008 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries
Internet

User and password are preset to

gwadmin

ETH1 IP is

192.168.1.42

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Setting the IP and CPAM on the GW module

DHCP is on by default

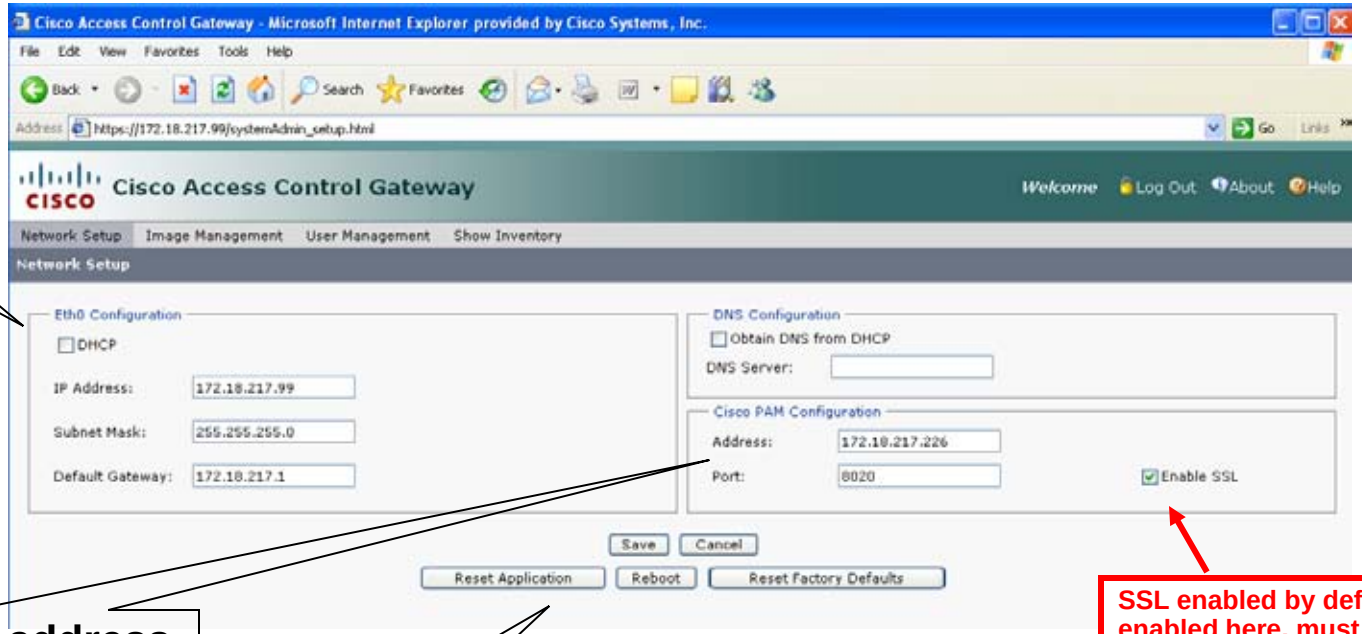
IP address

Mask

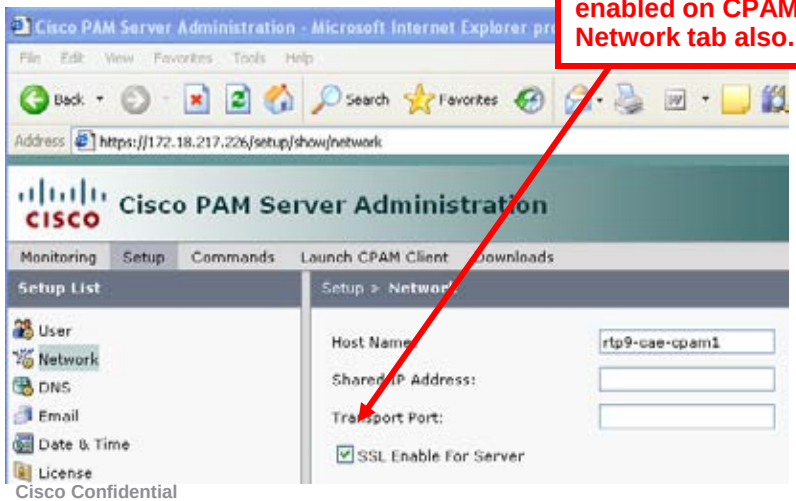
Default gateway

CPAM server IP address and port number

Gateway module Reboot, Reset to Factory Defaults, and Reset Application actions are also available.



SSL enabled by default. If enabled here, must be enabled on CPAM server Network tab also.

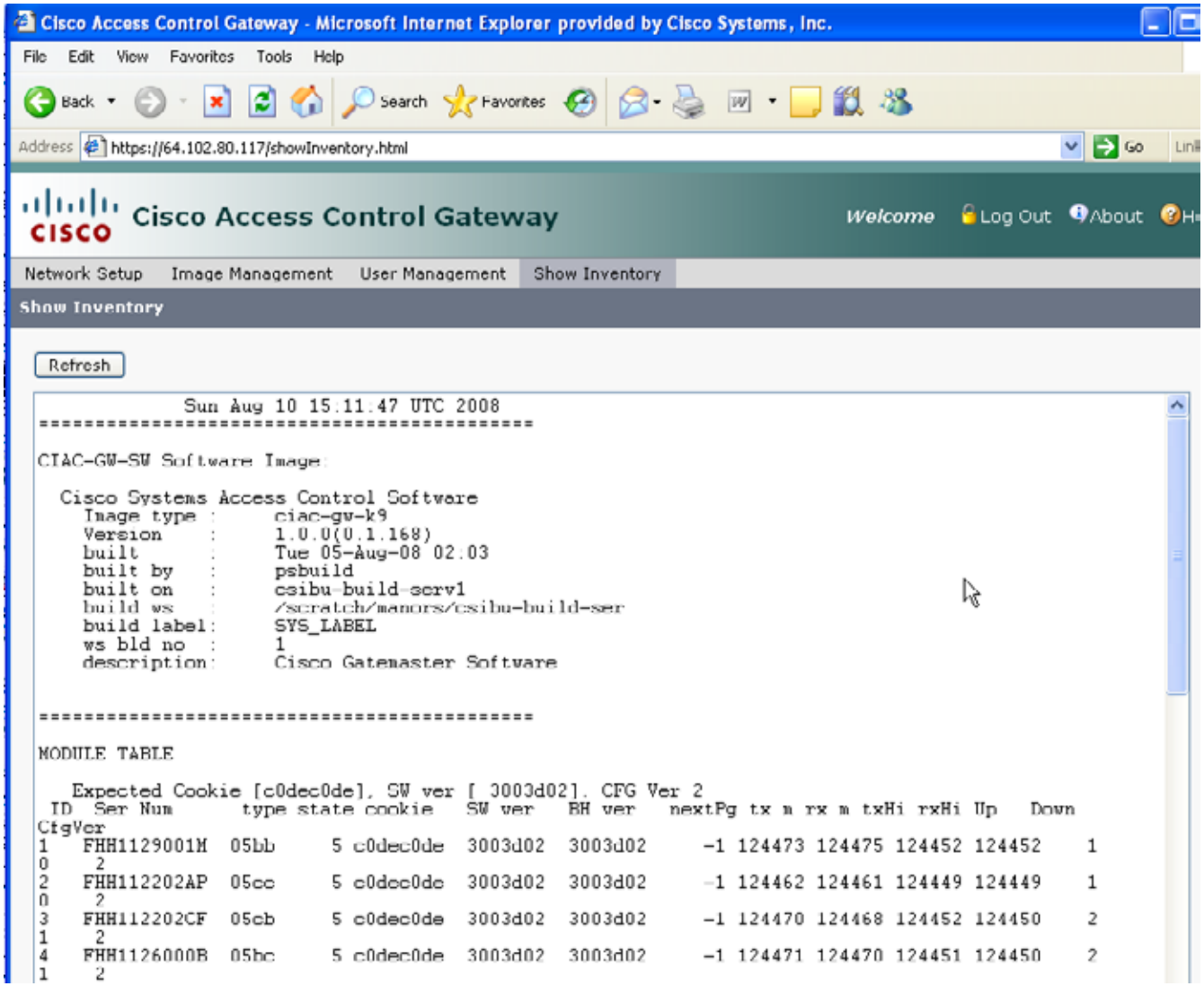


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Additional module inventory

Using the Show Inventory panel you can view status of the modules that are attached via the CAN bus.

You can scroll down and view specific information for each attached module.


Cisco Access Control Gateway - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://64.102.80.117/showInventory.html
Go
Cisco Access Control Gateway
Welcome
Log Out
About
Network Setup
Image Management
User Management
Show Inventory
Show Inventory
Refresh
Sun Aug 10 15:11:47 UTC 2008
CIAC-GW-SW Software Image:
Cisco Systems Access Control Software
Image type : ciac-gw-k9
Version : 1.0.0(0.1.168)
built : Tue 05-Aug-08 02.03
built by : psbuild
built on : csibu-build-serv1
build ws : /scratch/manors/csibu-build-ser
build label: SYS_LABEL
ws bld no : 1
description: Cisco Gatemaster Software
MODULE TABLE
Expected Cookie [c0dec0de], SW ver [3003d02], CFG Ver 2
ID Ser Num type state cookie SW ver HH ver nextPg tx m rx m txHi rxHi Up Down CfgVer
1 FHH1129001M 05bb 5 c0dec0de 3003d02 3003d02 -1 124473 124475 124452 124452 1 0 2
2 FHH112202AP 05cc 5 c0dec0de 3003d02 3003d02 -1 124462 124461 124449 124449 1 0 2
3 FHH112202CF 05cb 5 c0dec0de 3003d02 3003d02 -1 124470 124468 124452 124450 2 1 2
4 FHH1126000B 05bc 5 c0dec0de 3003d02 3003d02 -1 124471 124470 124451 124450 2 1 2

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

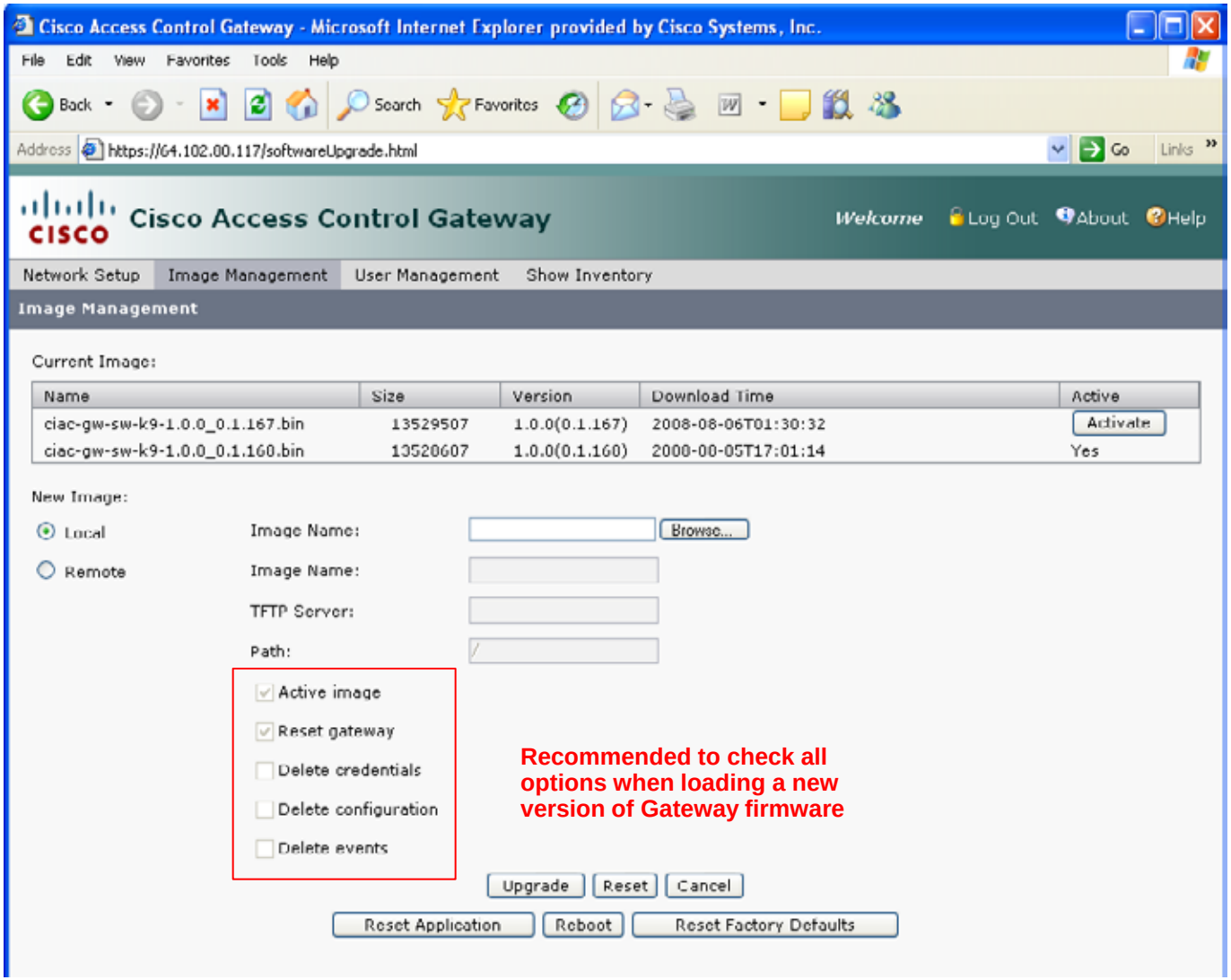
Gateway Image management

You can use the web interface to manage images on the Gateway,

Only non active image is overwritten.

Download occurs, then the you have the option to make the newly downloaded image the active image.

Once the new image is marked ‘active’ the next reboot will cause this image to be loaded and running.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

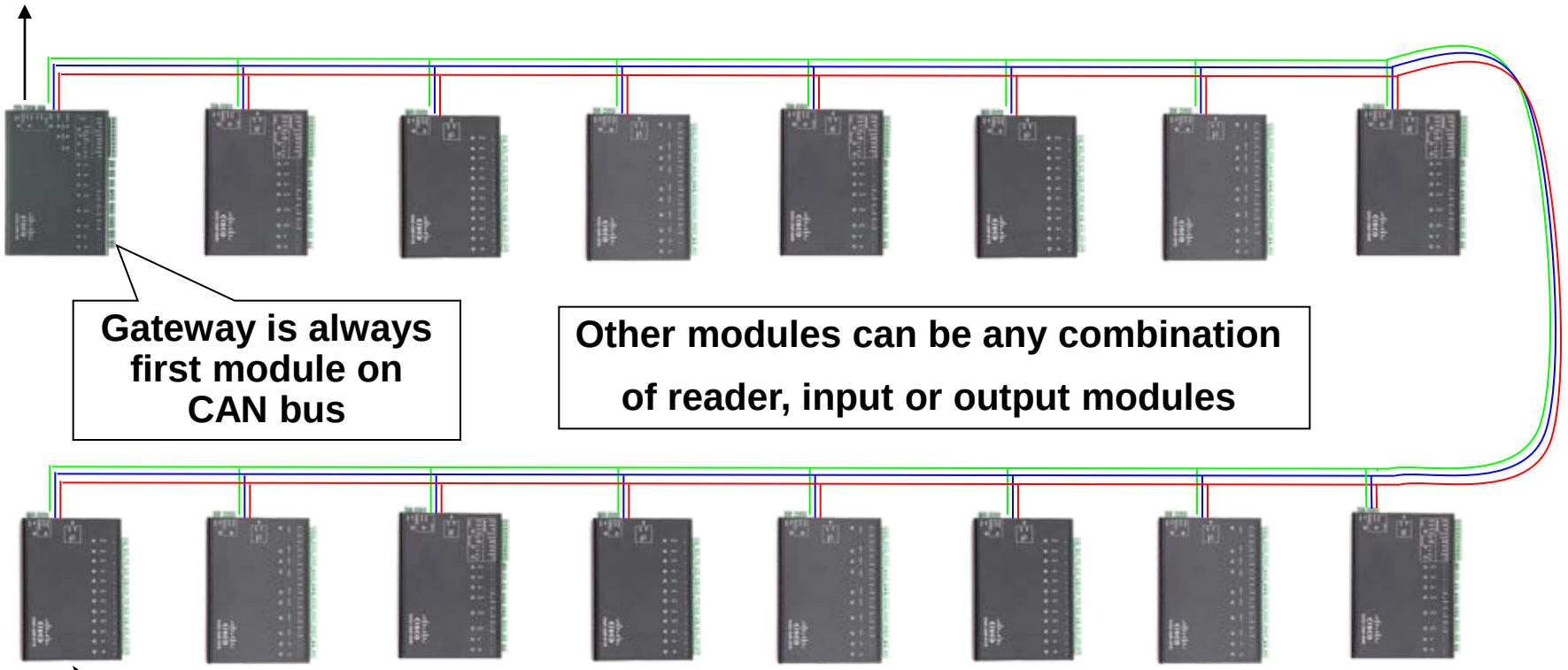
CAN bus

- Controller Area Network bus
- 3 wire, parallel bus connecting Gateway module to additional modules. (plus, minus, and shield)
- Must be terminated on both ends
- Gateway has CAN bus automatically terminated
- Last module (reader, input or output module) on bus must be set to terminate the CAN bus. This is manually configured with a switch setting on the module.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CAN bus layout

To IP network



Gateway is always first module on CAN bus

Other modules can be any combination of reader, input or output modules

CAN termination set on for this module and off for all other modules

MAX of 15 modules plus the gateway

Current speed 125bps

Current distance limit 1320 feet (400 Meters)

Verify CAN termination switch settings!

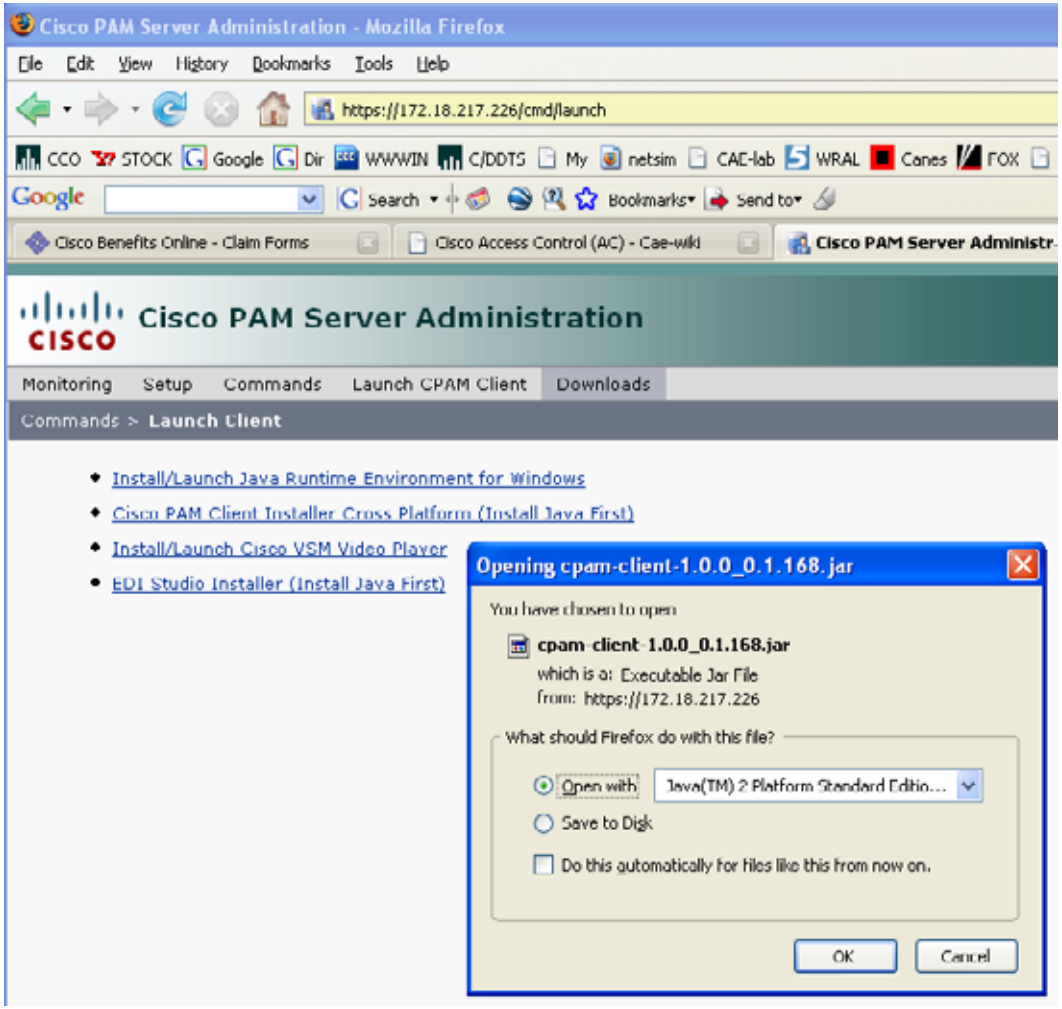
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CPAM client (configuring the hardware)

- Where do I get it from?
- Credential Templates (Card Formats)
- Device Templates
- Door Templates
- Gateway Templates
- Logical Door
- Locations
- Gateway image management via the client

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Where do I get this ‘client’?


Cisco PAM Server Administration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://172.18.217.226/cmd/launch
Cisco Benefits Online - Claim Forms
Cisco Access Control (AC) - Cae-wiki
Cisco PAM Server Administr
Cisco PAM Server Administration
Monitoring Setup Commands Launch CPAM Client Downloads
Commands > Launch Client
Install/Launch Java Runtime Environment for Windows
Cisco PAM Client Installer Cross Platform (Install Java First)
Install/Launch Cisco VSM Video Player
EDI Studio Installer (Install Java First)
Opening cpam-client-1.0.0_0.1.168.jar
You have chosen to open
cpam-client-1.0.0_0.1.168.jar
which is a: Executable Jar File
from: https://172.18.217.226
What should Firefox do with this file?
Open with
Save to Disk
Do this automatically for files like this from now on.
OK
Cancel

HTTPS into the CPAM server.

Under Downloads menu, click on

Cisco CPAM Client…

Or click on Launch Client

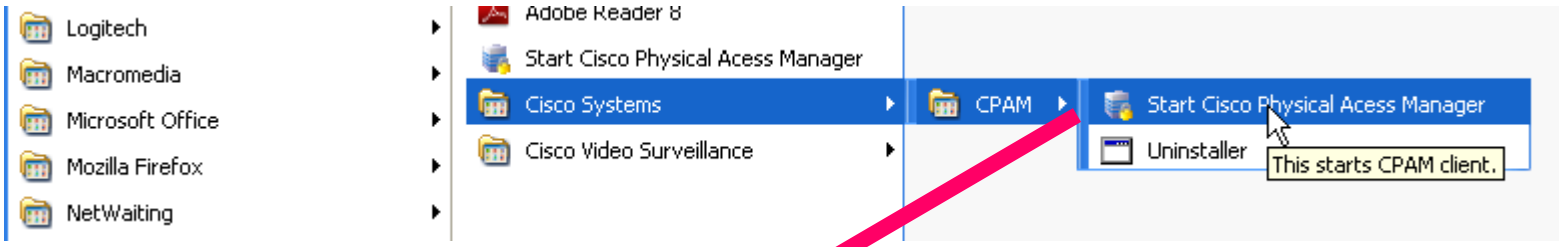
New versions can be installed over existing versions.

Required Java module is also available.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Log in via the client

Found under Programs, in the directory noted below.



Client login username and password will be provided by the CPAM server administrator.

This 'client' is used for all monitoring, and configuration.

Hardware configuration information is stored on the CPAM server, not on the client machine.

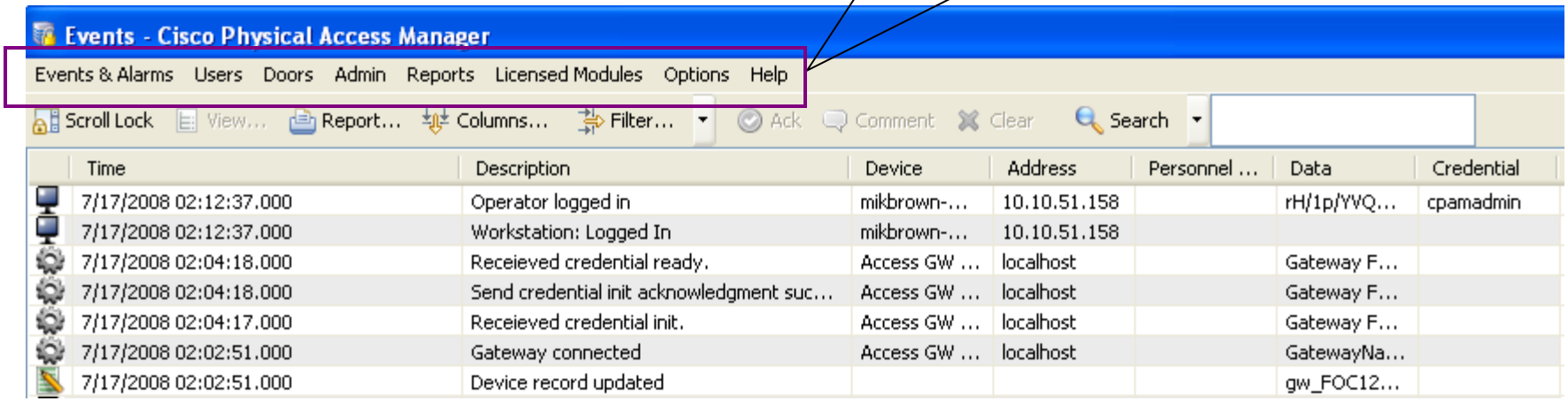
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Window jumping, from here to anywhere

Different application windows are used to monitor the hardware, perform hardware configuration, input users, and perform other tasks related to the Access Control solution.

This menu bar is available on each window that is opened. You can get to any window from any window.

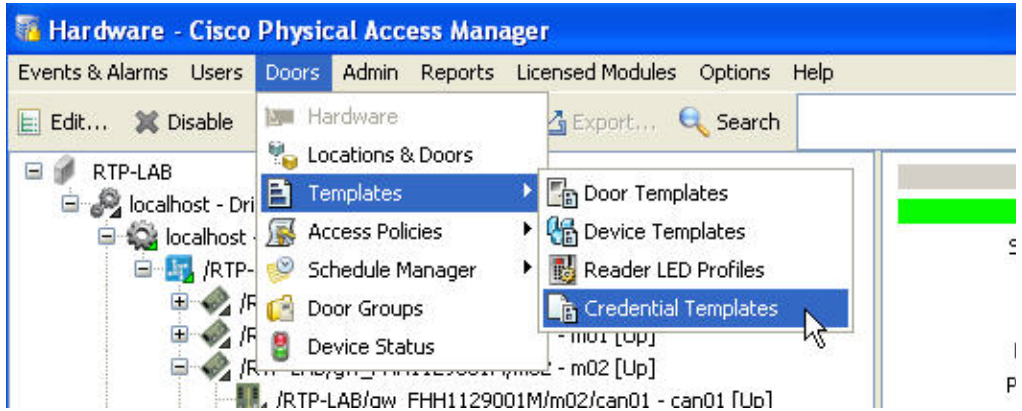
Only one instance of a window (single window instance) will be opened by default. Window behavior is configurable under system settings. Default is single window instance for each panel.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

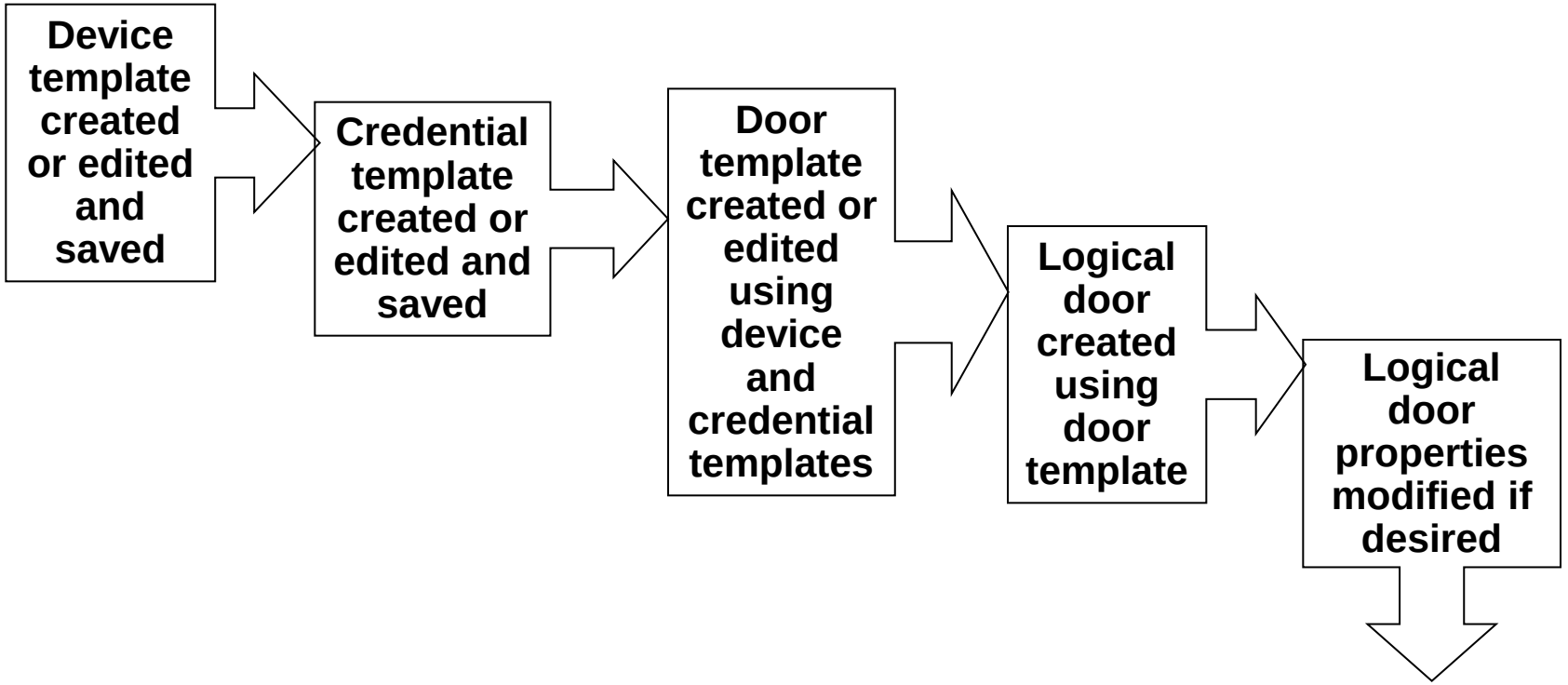
Templates

- Used for credentials, devices, doors, and gateways
- Samples of each type included with default configuration. Samples can not be modified.
- Customer can create their own templates
- Edits to customer generated templates **do** affect previously configured items, and will be used for any newly created items.
- Changes can be made on logical door and device items if the template was not exactly as desired.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

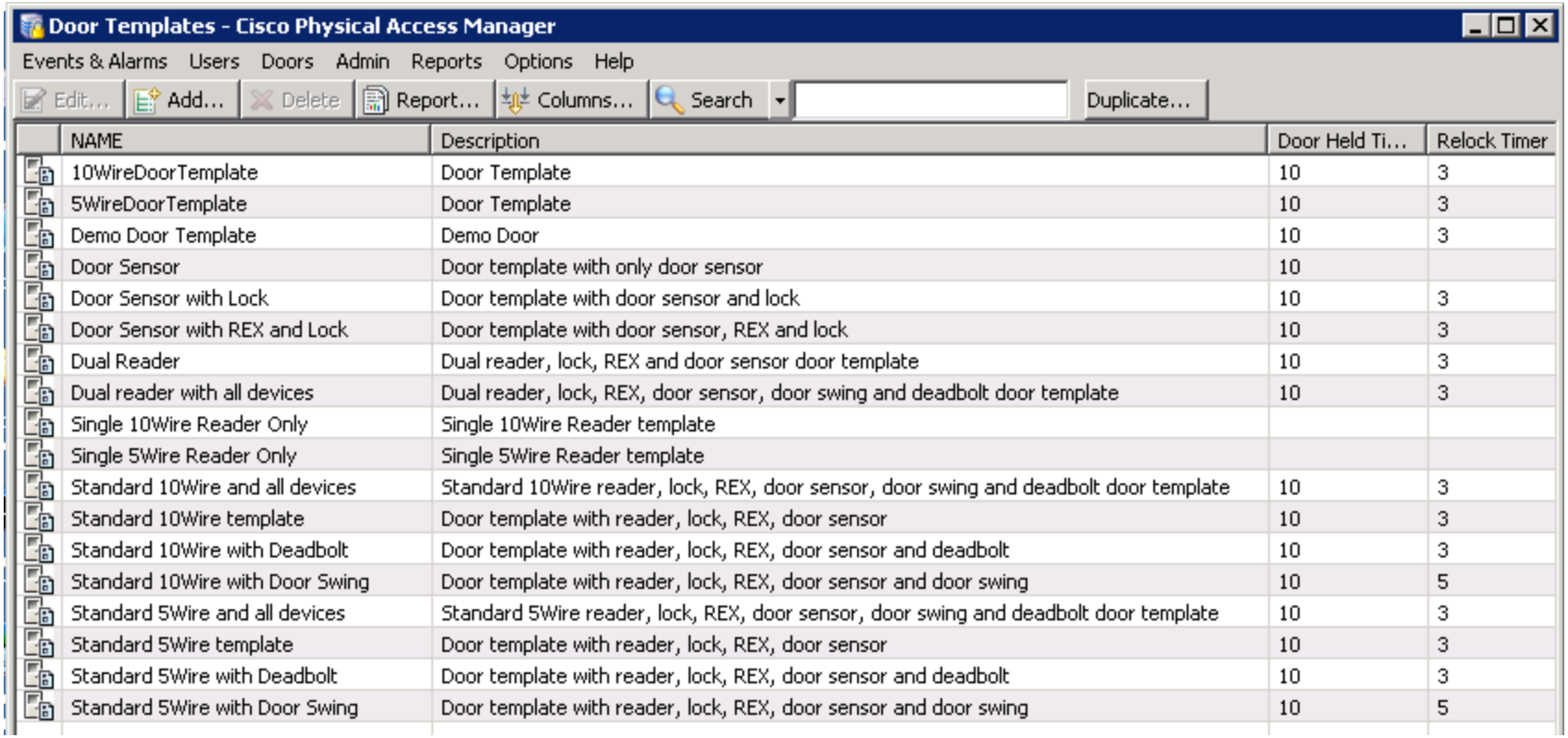
Templates


Device template created or edited and saved
Credential template created or edited and saved
Door template created or edited using device and credential templates
Logical door created using door template
Logical door properties modified if desired
Desired final configuration

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Flexible Door Template

- Doors templates can consist of any number of devices.
- Several Door Templates are pre-existing
- Custom Door Templates can be created as needed



NAME	Description	Door Held Ti...	Relock Timer
10WireDoorTemplate	Door Template	10	3
5WireDoorTemplate	Door Template	10	3
Demo Door Template	Demo Door	10	3
Door Sensor	Door template with only door sensor	10	
Door Sensor with Lock	Door template with door sensor and lock	10	3
Door Sensor with REX and Lock	Door template with door sensor, REX and lock	10	3
Dual Reader	Dual reader, lock, REX and door sensor door template	10	3
Dual reader with all devices	Dual reader, lock, REX, door sensor, door swing and deadbolt door template	10	3
Single 10Wire Reader Only	Single 10Wire Reader template		
Single 5Wire Reader Only	Single 5Wire Reader template		
Standard 10Wire and all devices	Standard 10Wire reader, lock, REX, door sensor, door swing and deadbolt door template	10	3
Standard 10Wire template	Door template with reader, lock, REX, door sensor	10	3
Standard 10Wire with Deadbolt	Door template with reader, lock, REX, door sensor and deadbolt	10	3
Standard 10Wire with Door Swing	Door template with reader, lock, REX, door sensor and door swing	10	5
Standard 5Wire and all devices	Standard 5Wire reader, lock, REX, door sensor, door swing and deadbolt door template	10	3
Standard 5Wire template	Door template with reader, lock, REX, door sensor	10	3
Standard 5Wire with Deadbolt	Door template with reader, lock, REX, door sensor and deadbolt	10	3
Standard 5Wire with Door Swing	Door template with reader, lock, REX, door sensor and door swing	10	5

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Template theory in use example

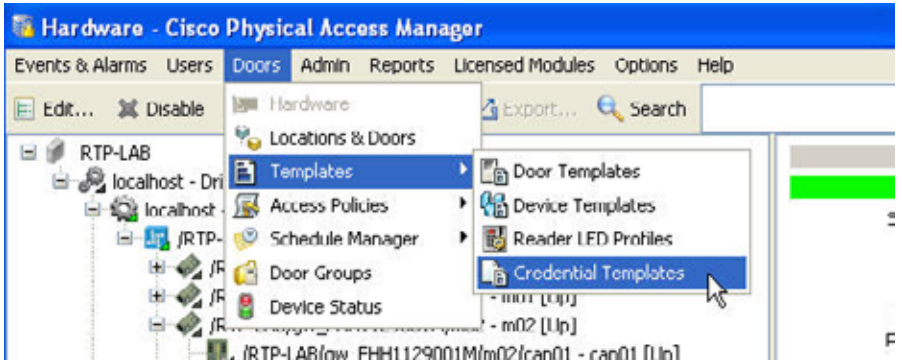
- You have 50 doors that will be configured.
- 1 of the doors will have a different REX operation than the other 49.
- Do I create 2 door templates?
- Or should I create 1 door template, use it for all 50 doors, and then on the 1 door with the different REX make the change on the logical door?
- Templates provide a set of default properties that can be changed as needed on the logical entity.
- If you have 25 doors with configuration A and 25 more with configuration B, you would create 2 different door templates.

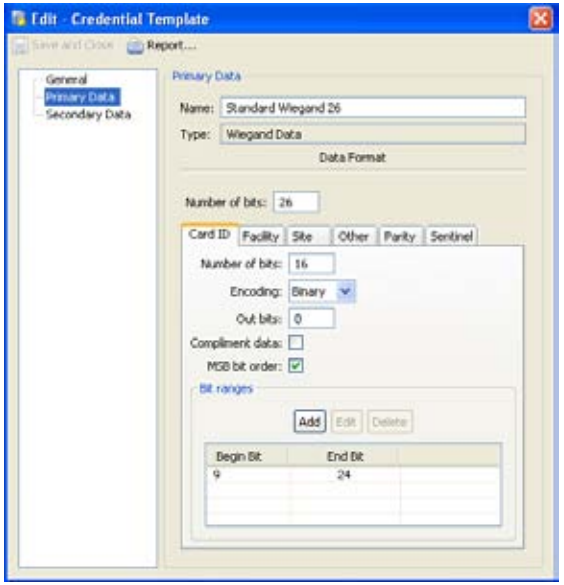
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

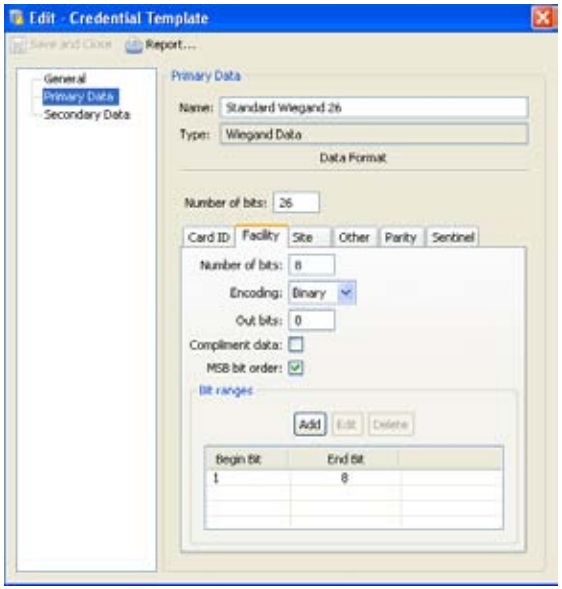
Credential template

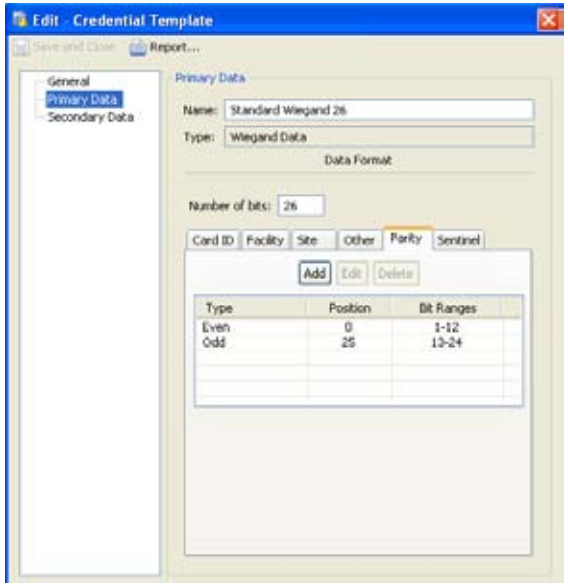
Card data must be obtained from the card provider.

No way to determine this information if it is not provided.







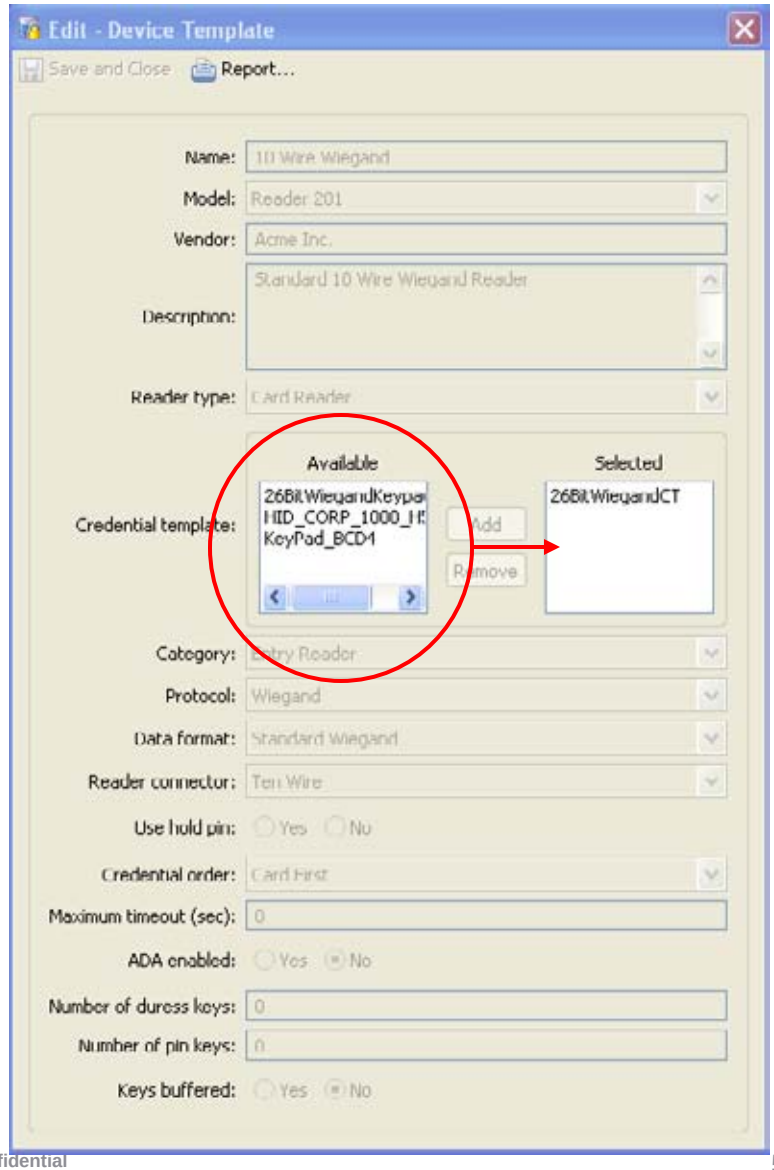


- **Credential template must match the bit lay out of the access cards being used.**
- **Total number of bits on card, and number of bits in each field must be configured.**
- **A begin and end bit position is needed for each field.**
- **If not configured correctly, the badge information can not be decoded and compared against the badge database correctly.**

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

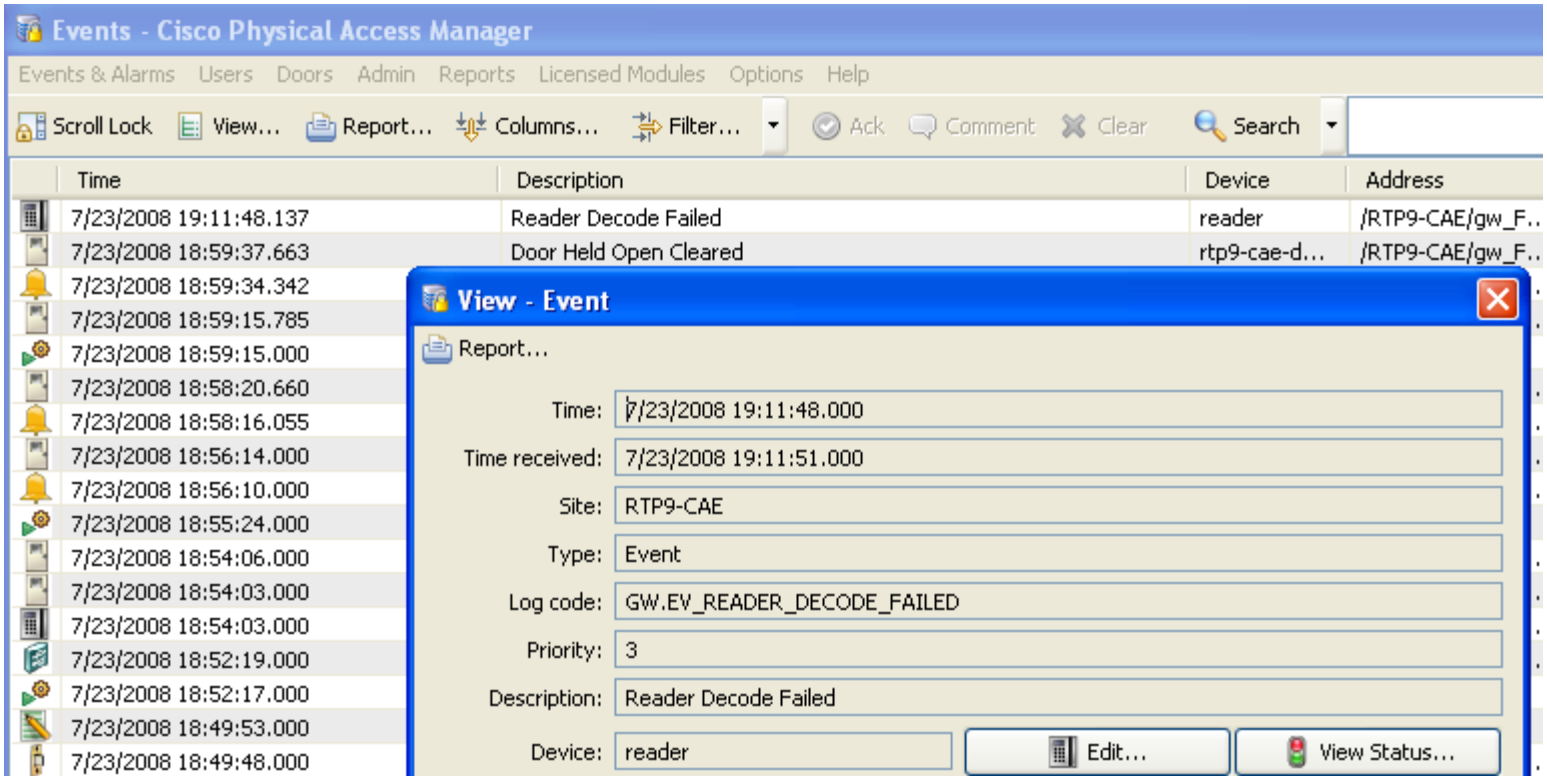
Associating Credential templates with reader

- Done on the reader device template.
- More than 1 credential template can be associated with the reader.
- ADA mode is for the Americans with Disabilities Act. This is used to configure a longer door open time to permit disabled individuals extra time to pass through the door.
- Specific badges can be flagged as ADA enabled, or the entire reader can be made ADA enabled.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What if the badge layout is unknown?

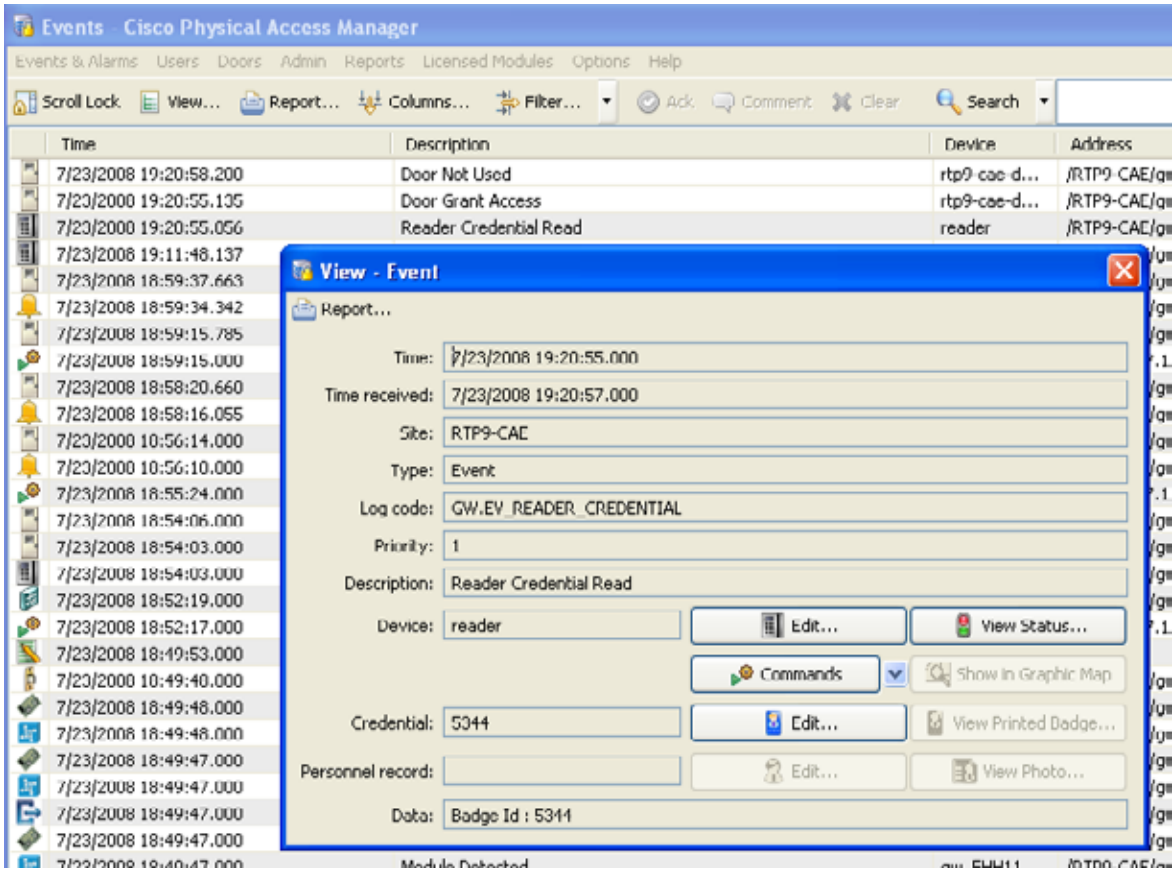


Reader Decode Failed message is posted…this indicates that the badge can be read, but the system does not know how to decode the bit layout on the card, so we can't identify the facility code or the badge number.

Could be that the Credential Template is incorrect for the badge presented, or that the badge layout does not match any of the current Credential Templates in use.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

If the badge is known!



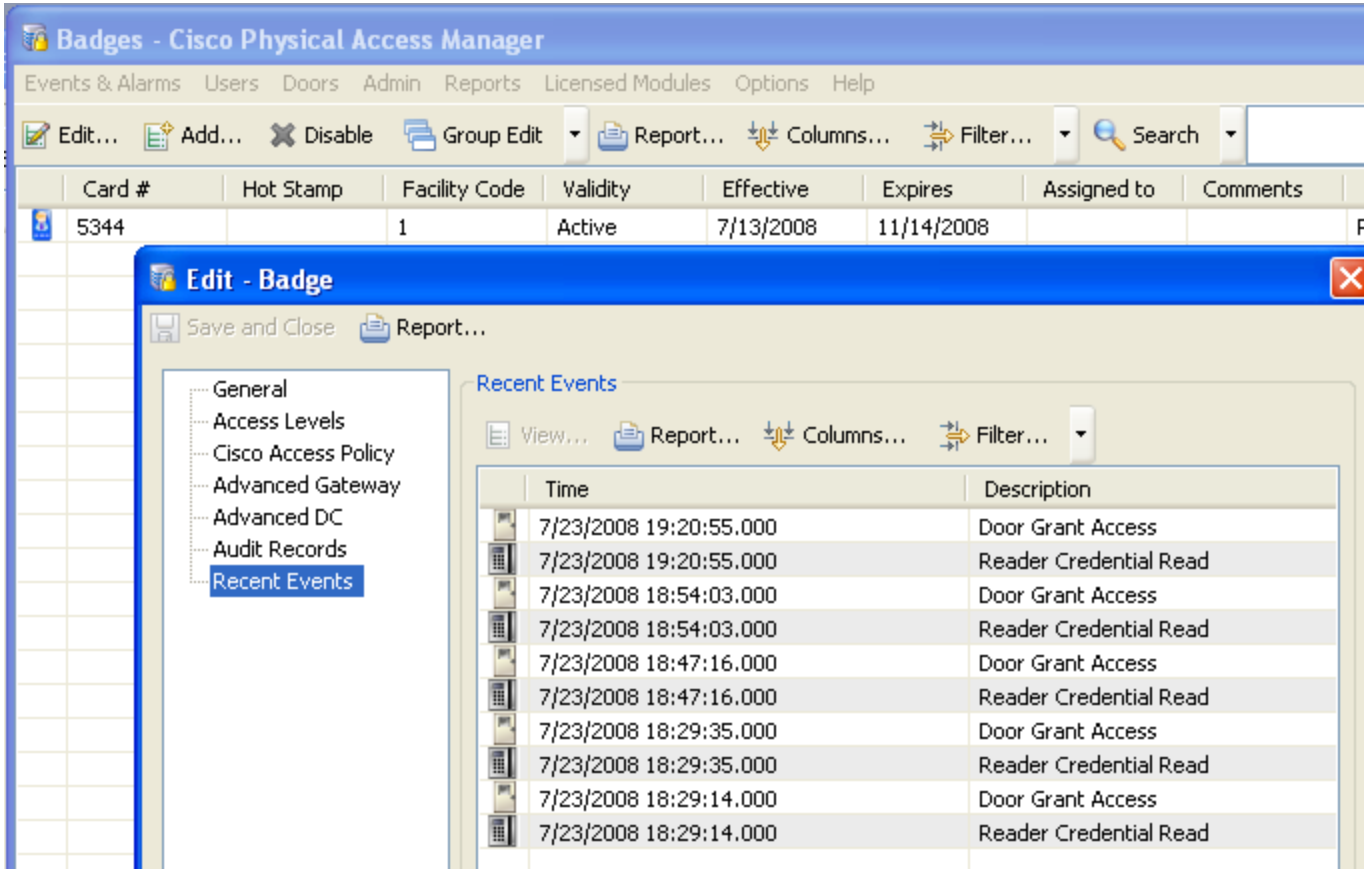
Badge number also displayed on the right side of the Door Grant Access entry.

Here we see that the badge was read and successfully decoded, and the door access was granted.

The badge number used was 5344. We can view statistics and audit records for that badge number in the badge database.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Audit trails

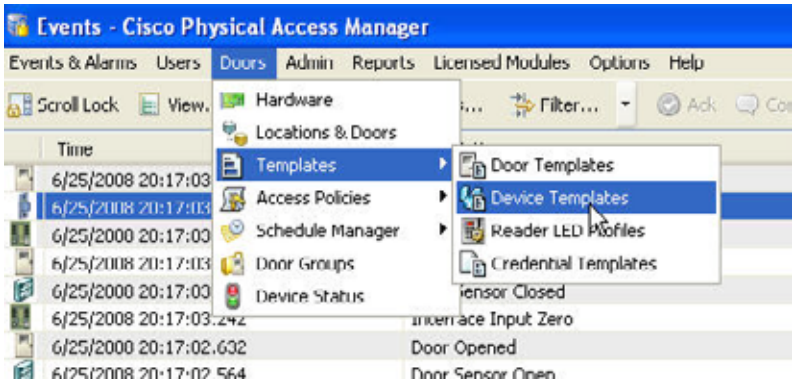


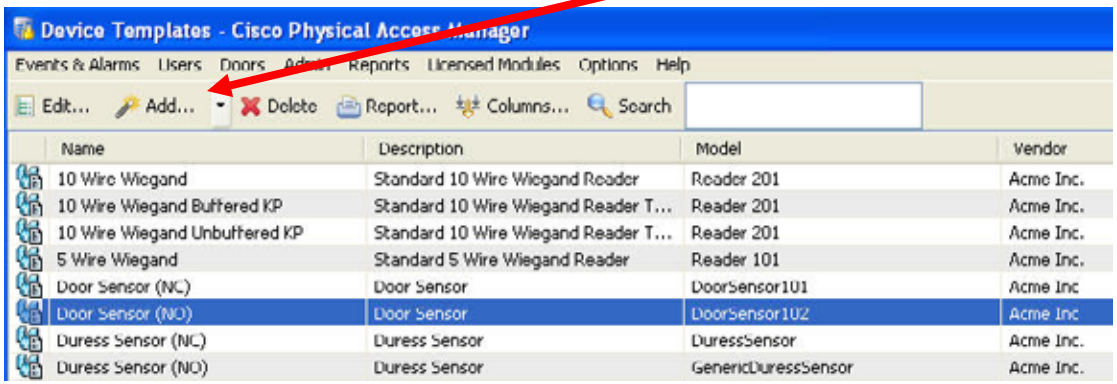
While viewing the badge record, we can look at Recent Events to see what the badge has done lately. If we high light the Door Grant Access at the top, we can see which specific door the badge was used at on 7/23/2008 at 19:20:55.000

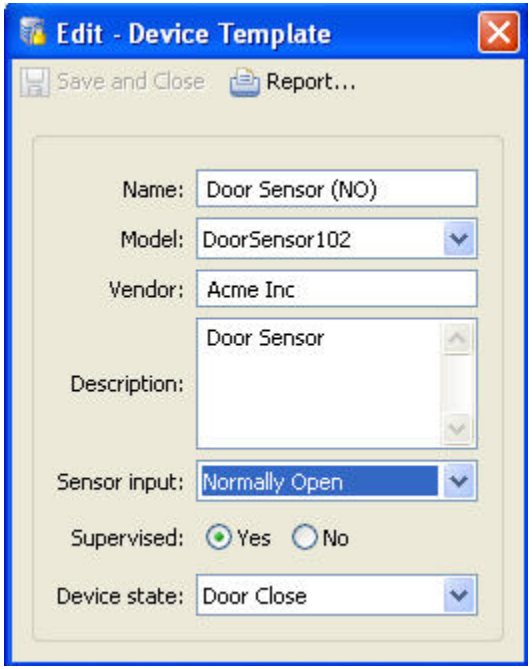
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Device templates (Inputs)

- Accessed from CPAM client main menu.
- Edit of existing device template is denied. Creation of new template is the way to configure unique operation.





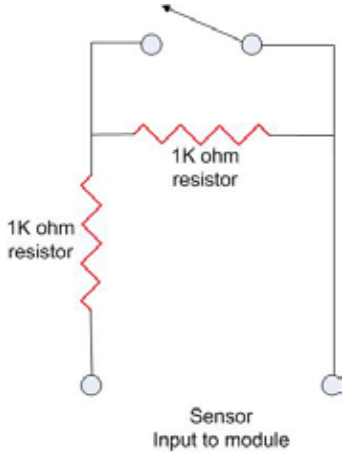


- Sensor input state: What is normal state of this device when not in the active state, it is open?
- Device state: What does it mean if this device is in the normal state, the door is closed.
- See next slide for details on supervised inputs.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is a supervised input?

- An unsupervised input has 2 states, active or inactive.
- Supervised input has 4 states, active, inactive, short, and open.
- Why do I care? What if a wire is cut or shorted between the module input and a normally open device. The server could not determine this and the device would remain in inactive state even when the switch is closed!
- How do I make the device/input supervised?
- Use 2 1K resistors in the circuit. In the inactive state, the circuit measures 2000 ohms, in the active state, the circuit measures 1000 ohms, short state would measure 0 ohms, and open state would measure infinite ohms. Now I can tell if a wire is cut or shorted

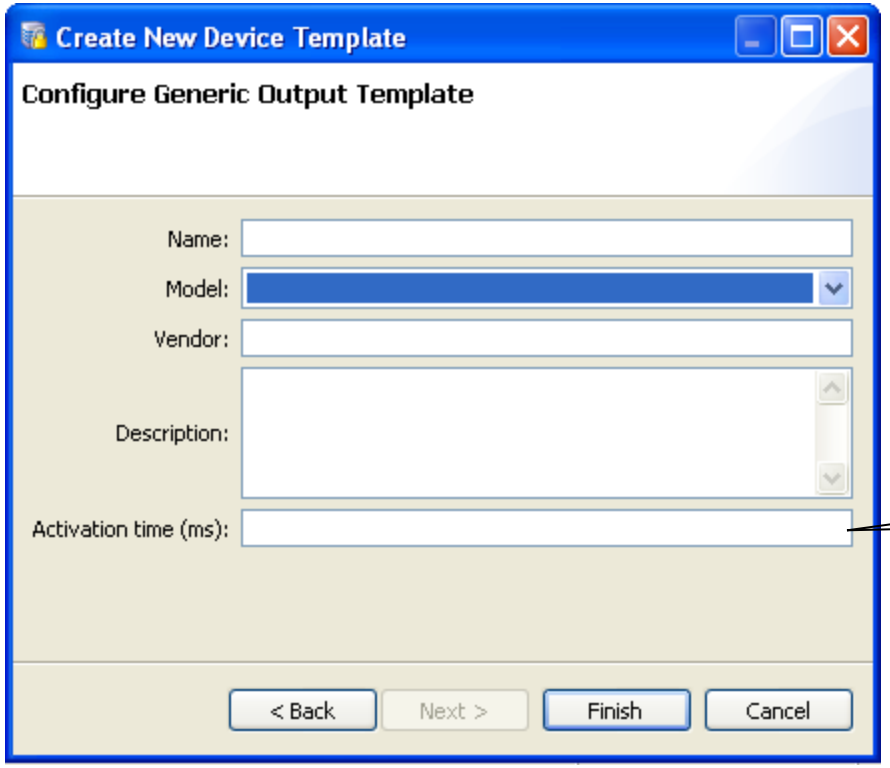


Example used: Door Sensor

OHMs	State	Door State	Error Posted?	Input Trusted?
2000	Inactive	Closed	No	Yes
1000	Active	Open	No	Yes
Zero	Short	?????	Yes	No
Infinite	Open	?????	Yes	No

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Generic Output



Creates from the Device Template main menu.

Not associated to a specific door.

Normally associated to a Global I/O or Device I/O action to be taken as a result of a trigger being detected.

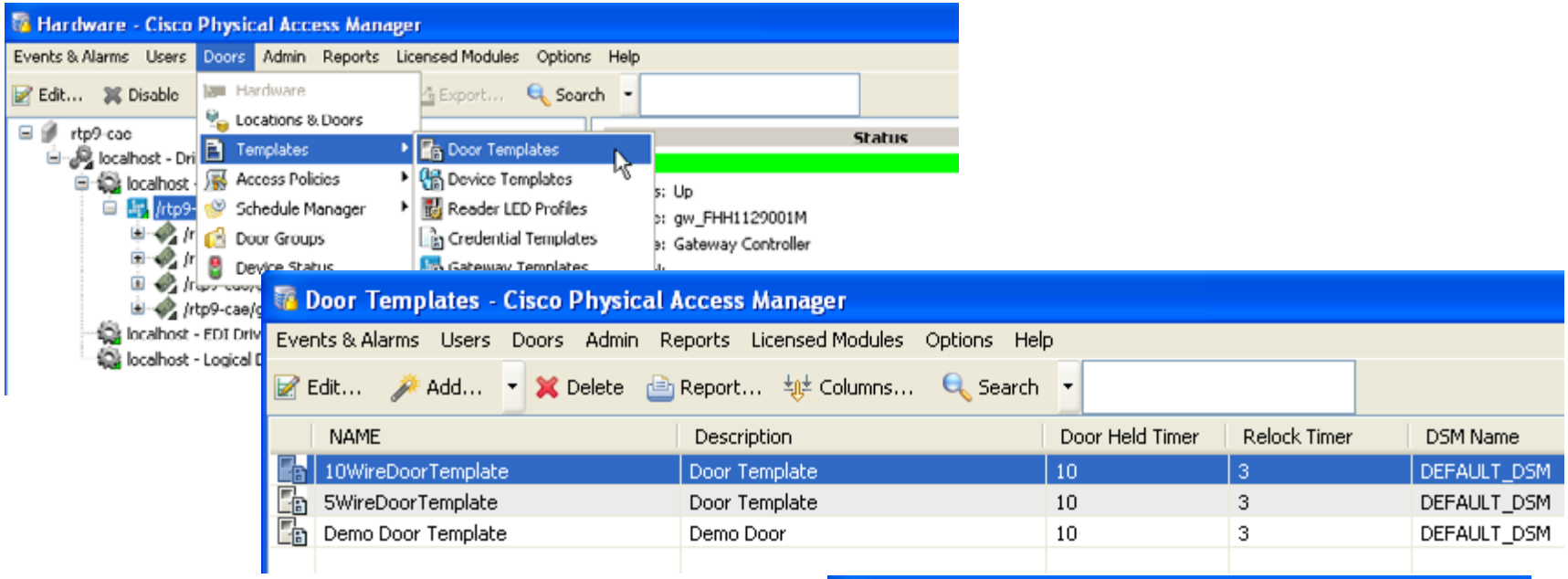
If the output is sent a 'timed activate' command, how long is the output to be in the activated state?

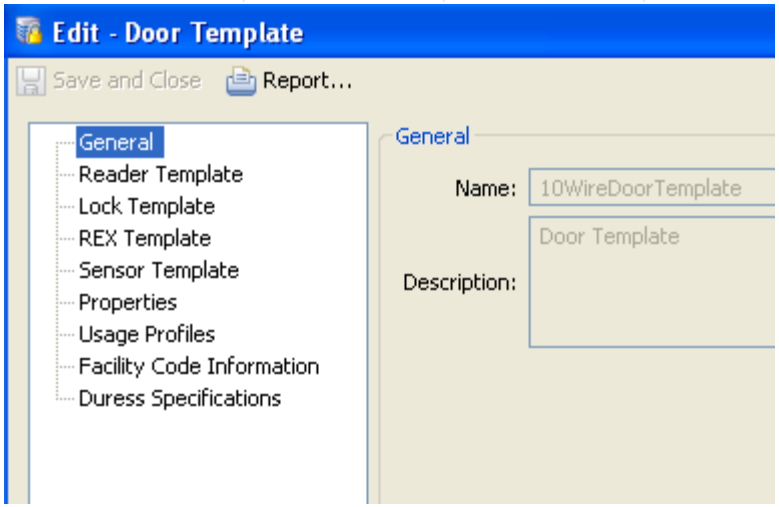
Example of use: If you want to turn on a light when an alarm condition exists. Wire the light circuit to the C and NO output connectors. Configure Global IO to use command 'Activate Relay' when the trigger is detected.

The relay will move from NO to Closed and complete the circuit, turning on the light, when the trigger is detected and the CPAM server initiates the 'action'.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Door Template





Used to create logical door layout. Each device points to a specific Device Template and inherits it operational characteristics from that Template.

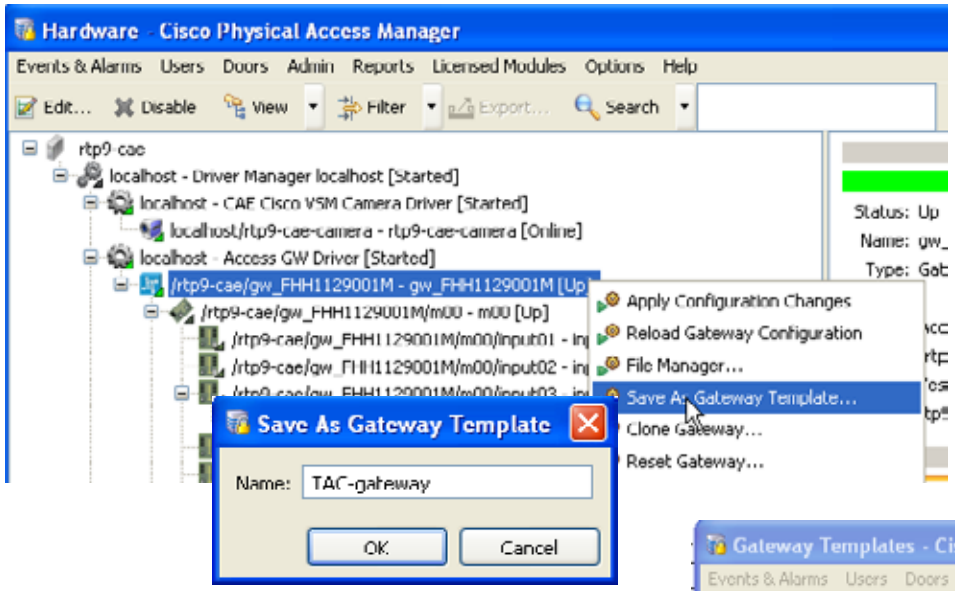
Predefined Door Templates can not be edited.

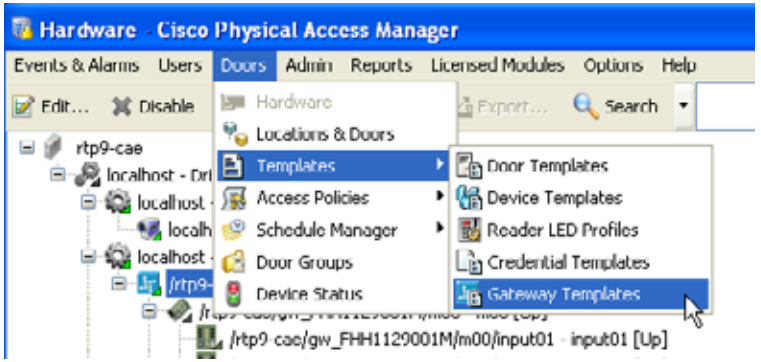
User can use these for input on how to generate Door Templates specific to their environment.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

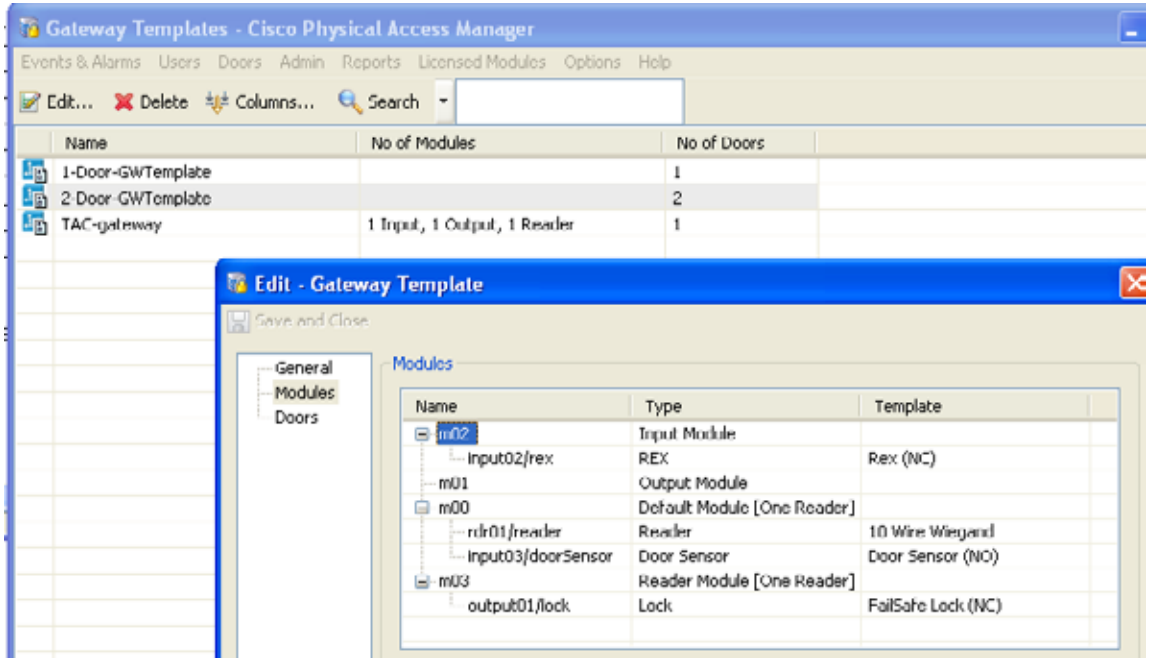
Gateway Template

Useful for multiple Gateways that will be configured with the same additional modules, and the same device attachment.


Hardware - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Licensed Modules Options Help
Edit... Disable View Filter Export... Search
rtp9-cae
localhost - Driver Manager localhost [Started]
localhost - CAE Cisco VSM Camera Driver [Started]
localhost/rtp9-cae-camera - rtp9-cae-camera [Online]
localhost - Access GW Driver [Started]
/rtp9-cae/gw_FHH1129001M - gw_FHH1129001M [Up]
/rtp9-cae/gw_FHH1129001M/m00 - m00 [Up]
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
Clone Gateway...
Reset Gateway...
Save As Gateway Template
Name: TAC-gateway
OK
Cancel

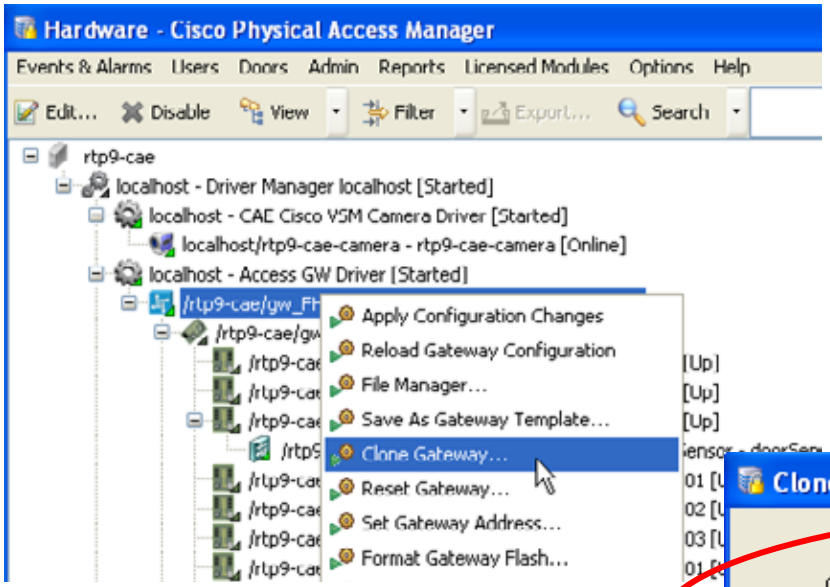


Once you have a Gateway configured the way you want, you can save the configuration as a Gateway Template. When you add additional Gateway modules, you can use the template to populate the configuration for that Gateway and associated modules.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

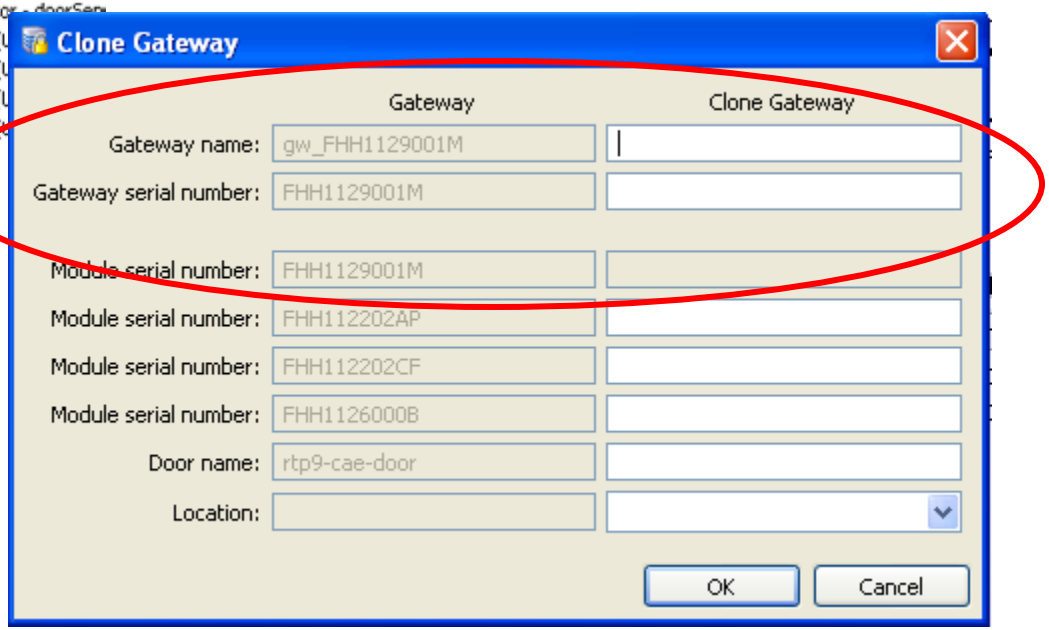
Gateway Cloning



Useful when you are pre-provisioning the CPAM server for future Gateways that will be added. If the Gateway is standalone, the 3 additional modules seen in this example would not be shown. This generates a new Gateway configuration, along with associated module, that is identical to the Gateway being cloned. You must have the Gateway and additional module serial numbers handy to use this feature.

For single Gateway cloning, all you need is the Serial number, and a unique name

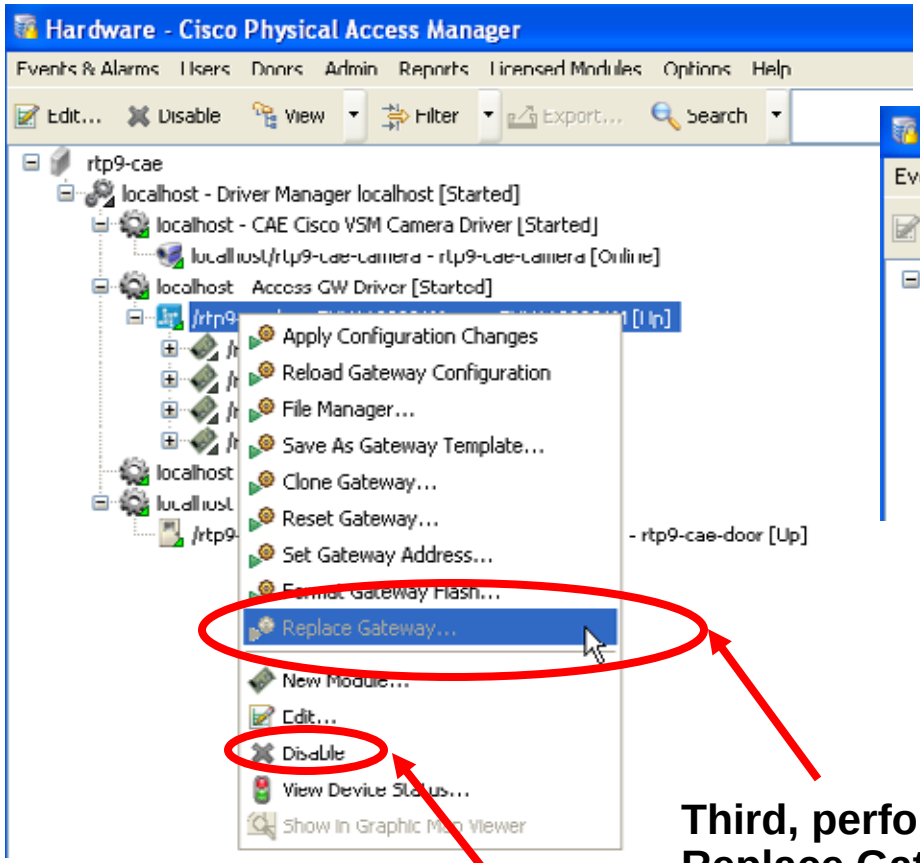
Big difference between gateway template and cloning is that the cloning includes all the configuration associated including doors, access policies etc related to doors on that gateway. Gateway template consists of only the interface to device/device template information



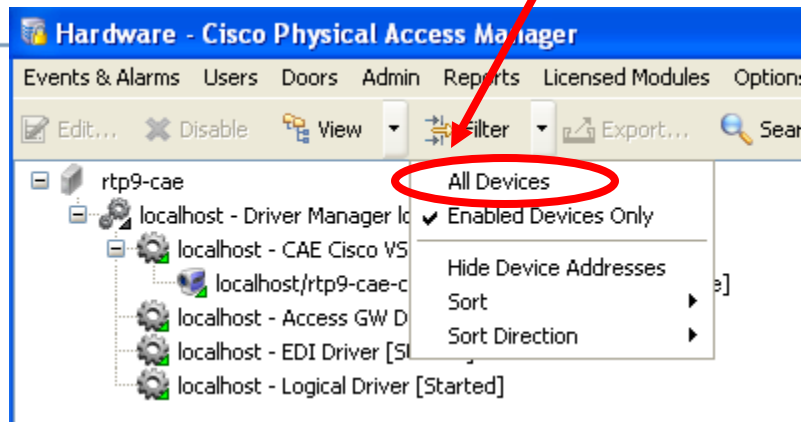
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Gateway module replacement

All devices controlled by the Gateway should be disabled prior to starting the Gateway Replacement process



Second, set display filter to All Devices



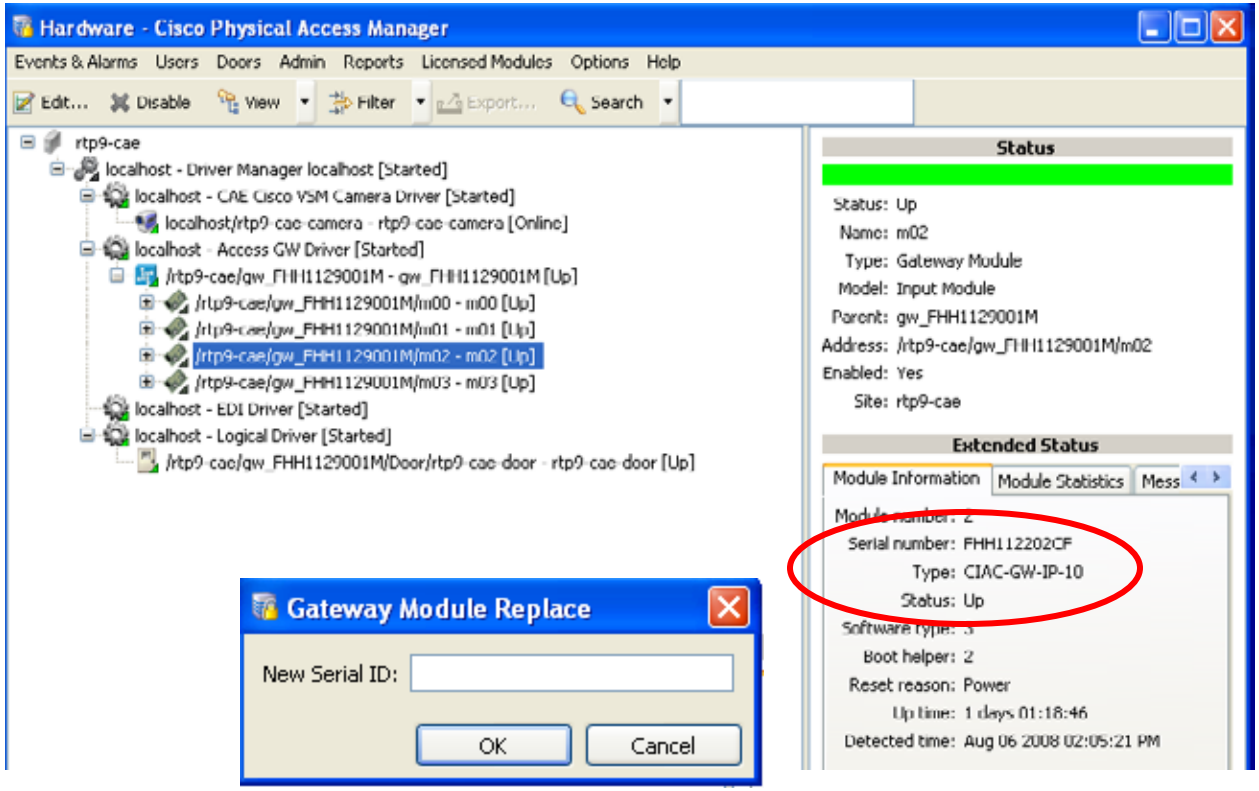
Third, perform Replace Gateway

First, Disable the Gateway

At this point you should see the Gateway in the Hardware Tree as Disabled, and if you right click on the Gateway, the Replace Gateway option should be enabled.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Replace non Gateway module



On the client, Hardware tree display, right click on the module being replaced.

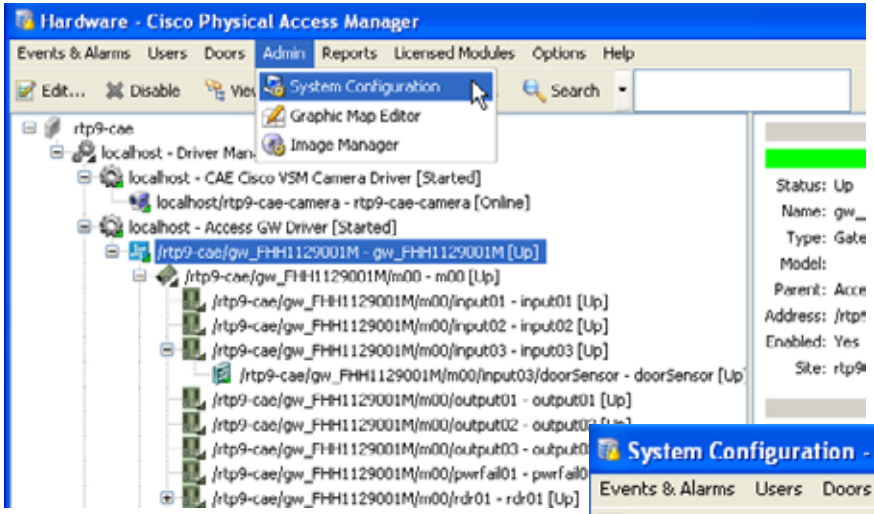
Left Click on the Replace Module option.

Key in the new serial, and click OK

You can now move the power, CAN bus, and device connections to the new module.

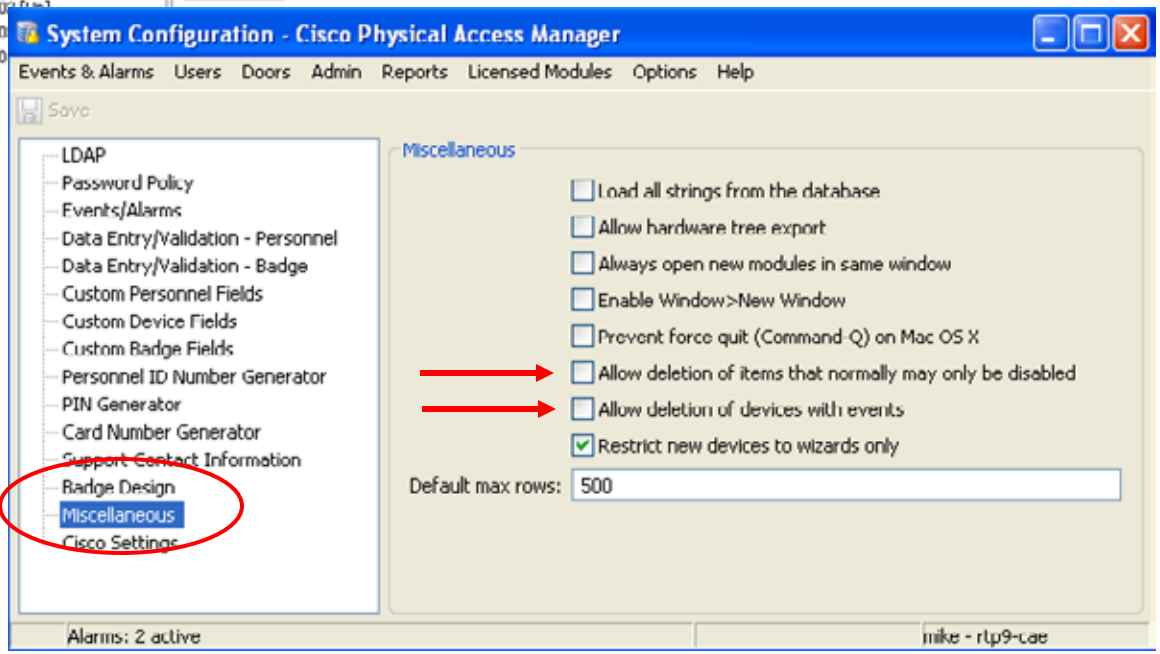
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Disable/Delete function



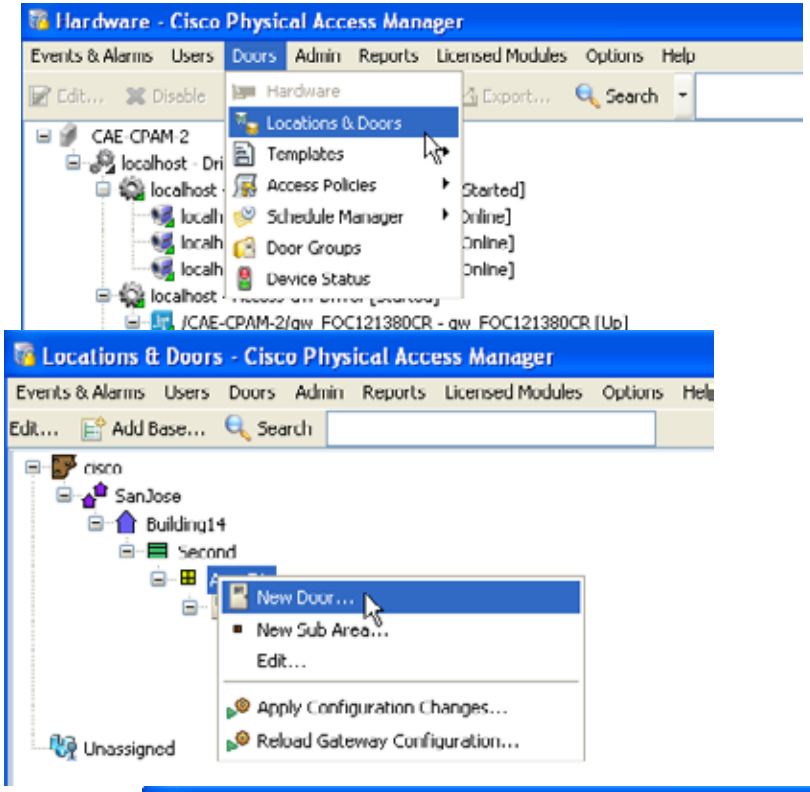
By default, devices can only be disabled, not deleted. If the customer wishes to be able to delete items from the configuration, then they must enable the function.

Making changes to the System Configuration requires a STOP and START be issued on the CPAM application from the Web administration interface.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Creating the Door

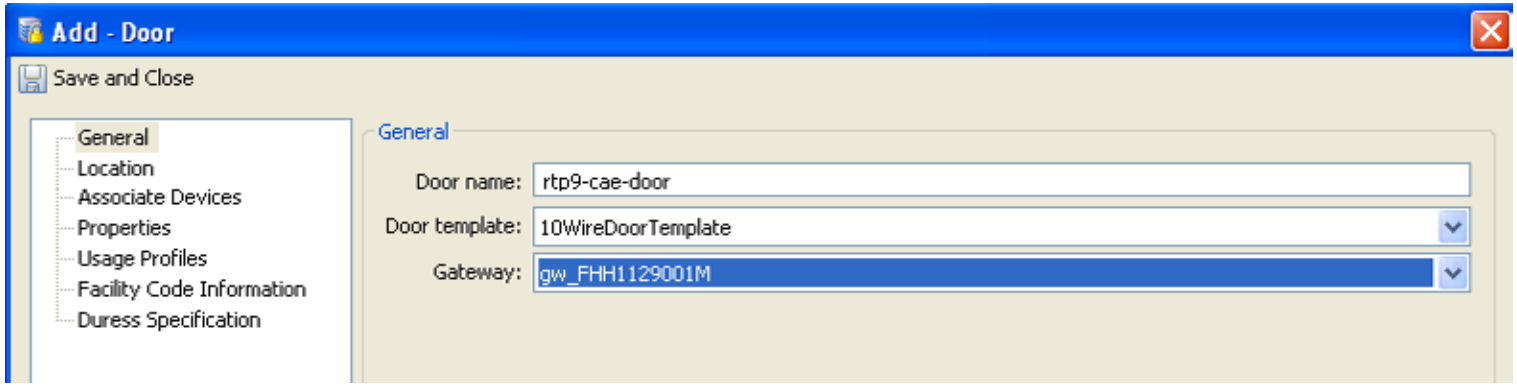


Logical door is created under the Locations & Doors tab.

You name the door (must be unique to location)

You specify the Door Template to use.

You specify which Gateway will be used to monitor/control the devices associated with the door. Devices could be attached to modules via the CAN bus to the Gateway specified.



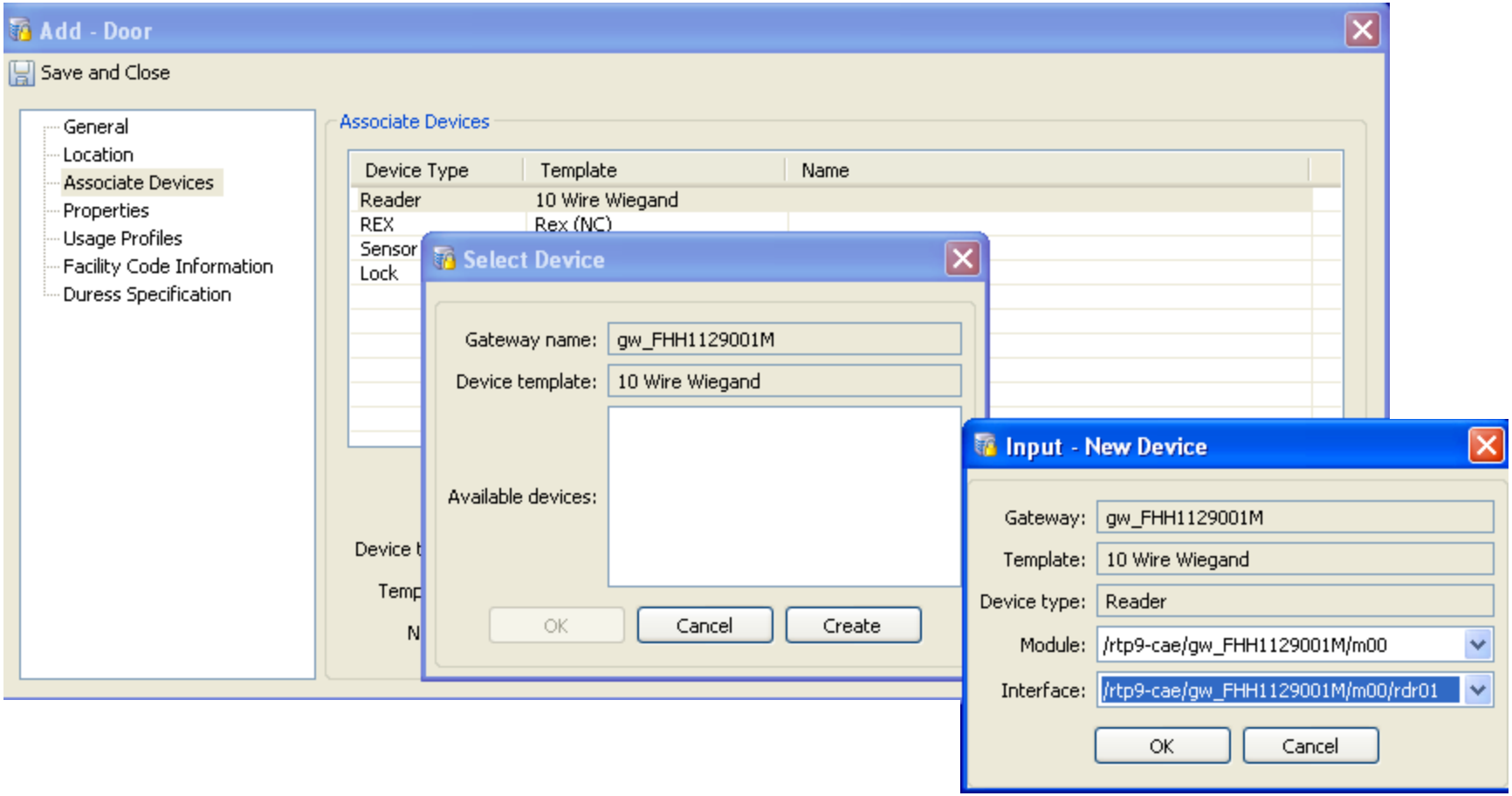
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The door theory!

- Basic door has 4 devices involved
- **The reader**…reads the badges presented and transfers decoded bit stream to gateway where gateway module or CPAM server decides whether to grant access or not.
- **Door sensor**… what position is the door in? Is it open or closed?
- **Rex**… request to exit. If the door opens, was it forced open or is someone leaving from secure side? The Rex lets us know the door was not 'forced open'.
- **The lock**…Once a valid badge is presented, the door has to be unlocked. Depending on the lock is wired to the Output, the module will open the circuit (C & NC) or close the circuit (C & NO)
- Some doors may have additional devices like a second reader to be used by ADA personnel. This reader might provide extra time for the people moving through the door.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

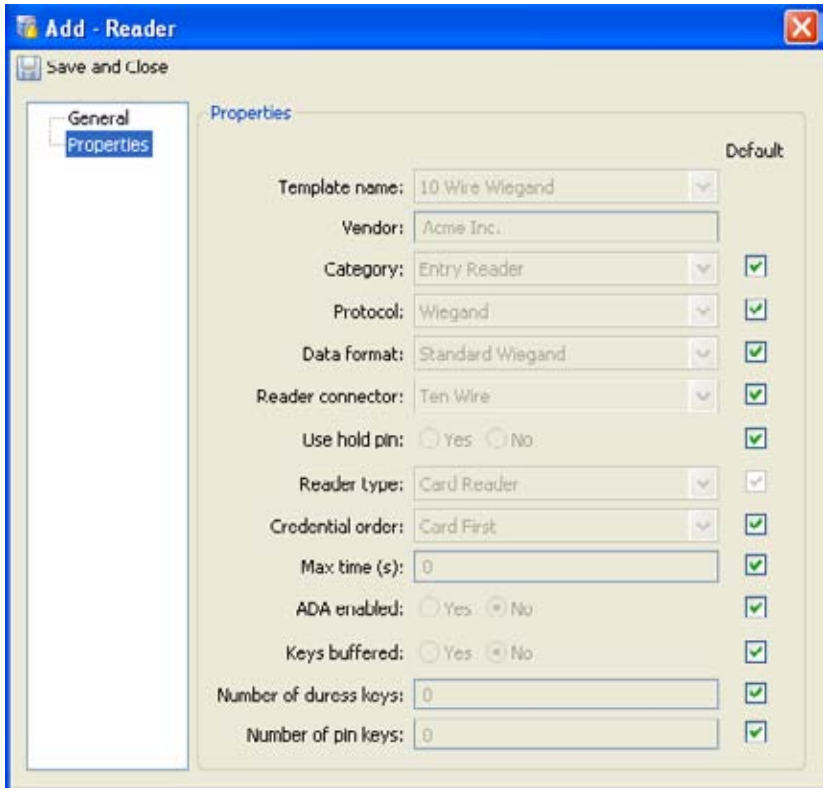
Door Device Associations



Under Associate Devices, you select the device type, and then associate that device with a specific module (list is based on the Gateway selected under the General tab) and specific interface on that module.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Deviations from the Templates



The device template used in the door template will dictate what the default behavior is.

If this specific door requires deviation from the device template, you can uncheck the default box and make the edit here.

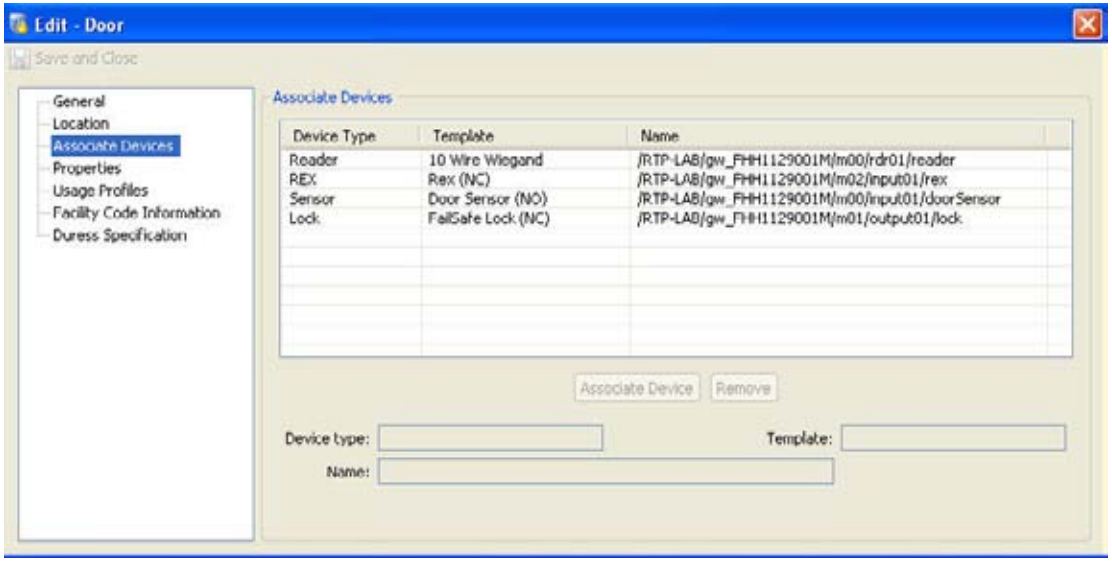
This does not alter the template.

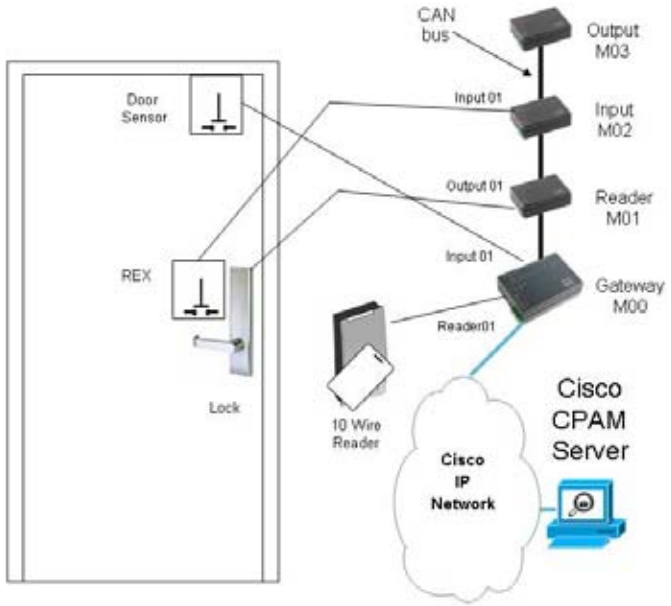
When completed with any edits, click on Save and Close.

Each device must be added in the same fashion.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logical door device associations

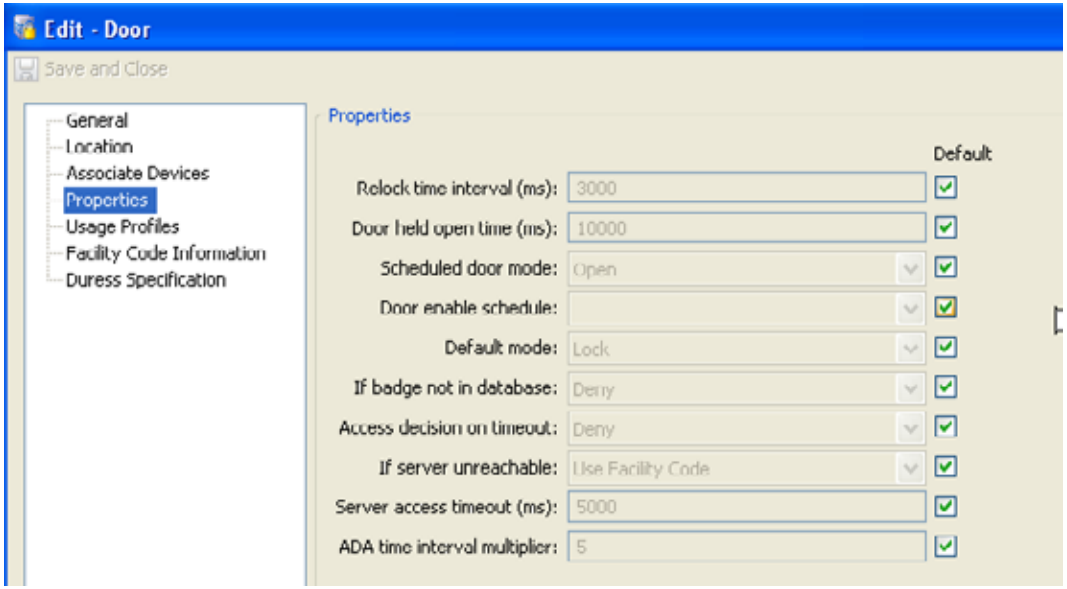




- Here is where we map the physical door connections to the hardware modules
- The reader is on M00, the gateway module in reader 1 position.
- The REX is on an Input module M02, in the input 1 position
- The door sensor is on the gateway M00, in the input 1 position
- The lock is on an output module M01, in the output 1 position

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Door properties (defaults are based on door template used to create the door)



Defaults are based on what is configured in the door template. Changes on this panel do not alter the template, only the operation of this specific door.

Relock time – Once opened by valid badge, how long is lock held open

Held open timer - how long can door stay open after valid user passing through before alarm is posted advising that the door did not close.

What happens if badge is not in database?

Access on timeout? I can reach CPAM, but it doesn't answer!

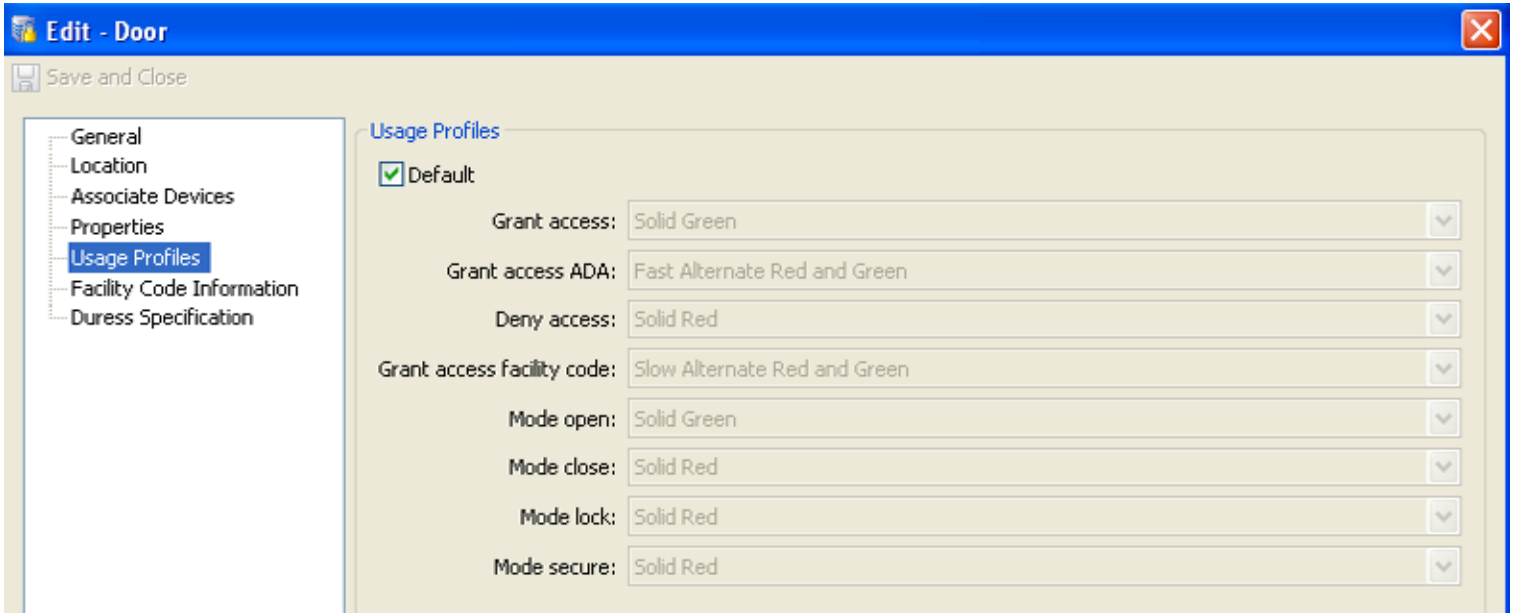
What to do if server is unreachable?

How long to wait for server response.

If badge is ADA enabled, multiply relock and held open timers by this number

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Door Usage Profile



Default is based on door template used to create the door.

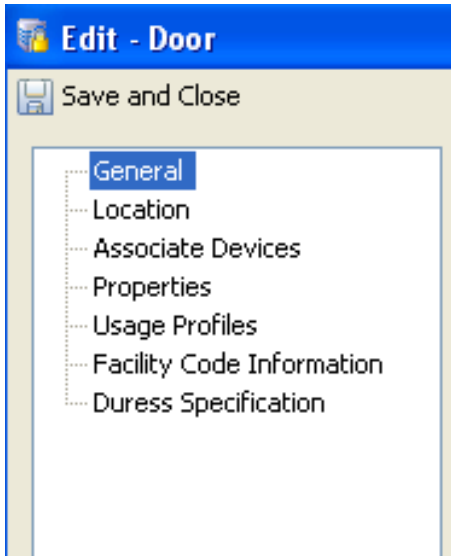
Changes here do not affect the door template, just this specific door/reader

The profile dictates how the LEDs on the reader device will operate.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Facility Code and Duress Specification

Credential templates are mapped to the door. What type of badges will be used to access this door. The readers have to be configured to decode the bits on the badge. Decisions can be made using the facility code. IE: for an outdoor restroom at the company recreation facility…do we really care who enters? We can configure the door to open if any badge with a specific facility code is presented. IE: any company badge can open the door.



Duress Specification is used to enable a person to signal for help when using a key pad for entry, with out alerting anyone near them.

Assume the duress code is 8

If a user is being coerced into opening a door, and their PIN is 1234x, if they enter 12348 as the PIN, the door will open and a message will be posted to the site security that a duress code was used. It provides a silent alert that the door was not opened under normal circumstances even though a valid badge and PIN were used.

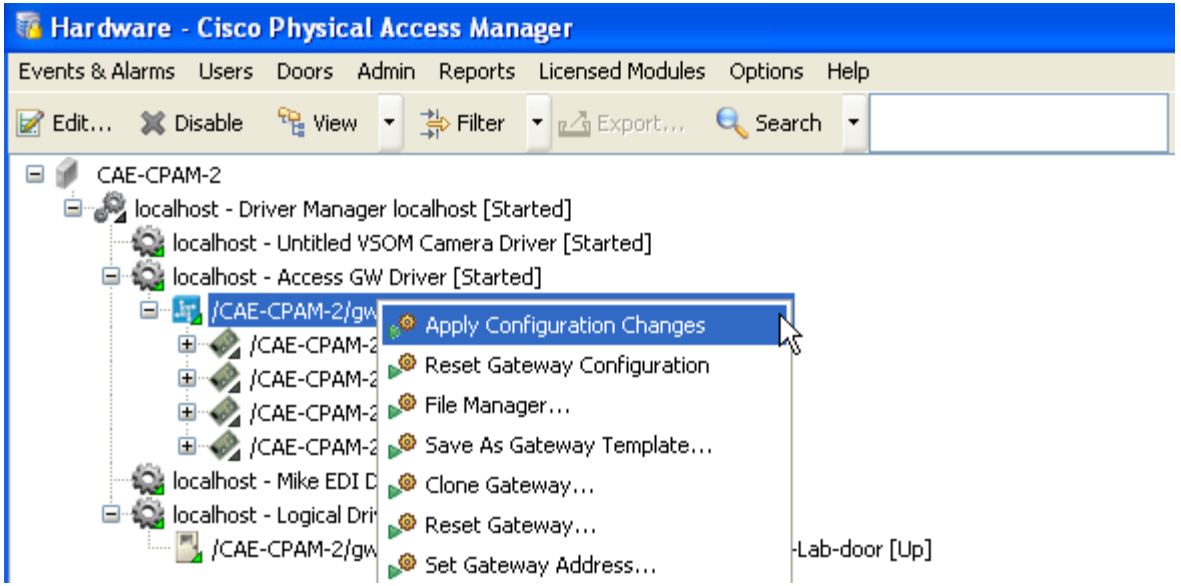
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuration download to the gateway

- Once the devices and doors are configured via the client, the configuration needs to be pushed to the gateway.
- Check properties, specify time zone then commit your changes.

Apply configuration changes - only sends the "Full" configuration the first time configuration is sent to the gateway - otherwise it sends delta changes.

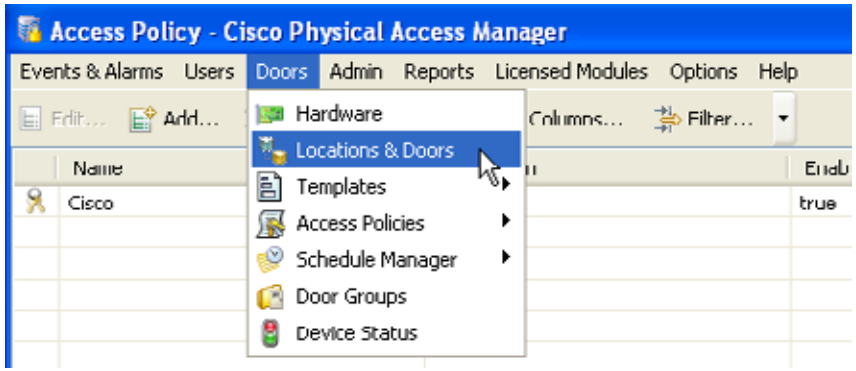
Consequently the gateway will reload only the first time configuration is applied.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logical device locations

- Easy way to determine what devices for a door are attached to what module
- Edits to devices and doors can made directly from this tree
- Changes made here do not affect device or door templates



Hierarchal tree of

base =>

campus=>

building=>

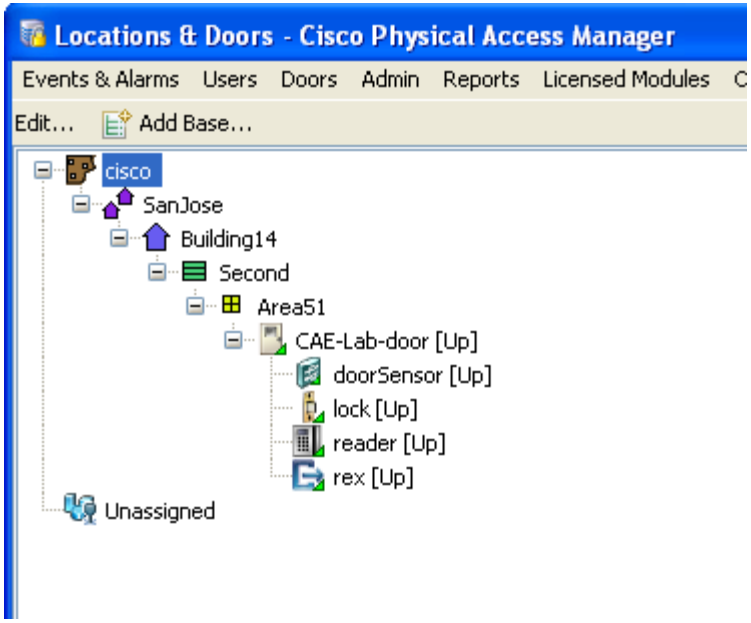
floor=>

area=>

sub-area=>

door=>

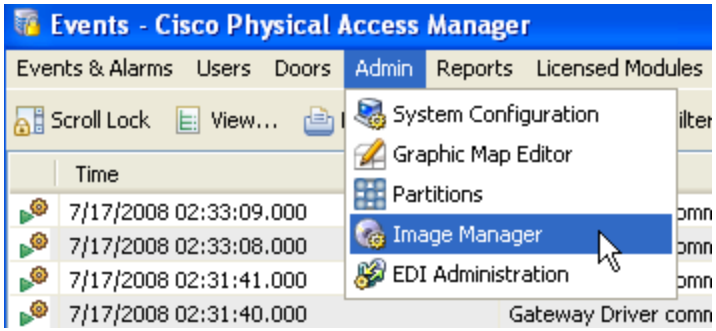
devices

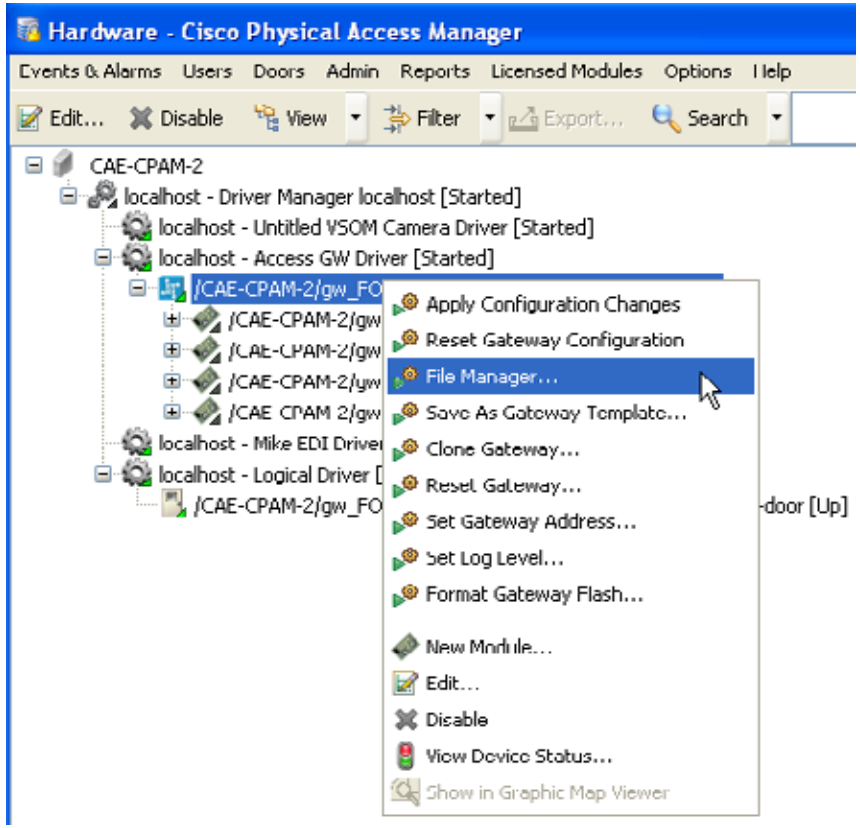


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firmware upgrades for Gateway module

- 2 step process…image file is uploaded from client machine to CPAM server using ‘Image Manager’





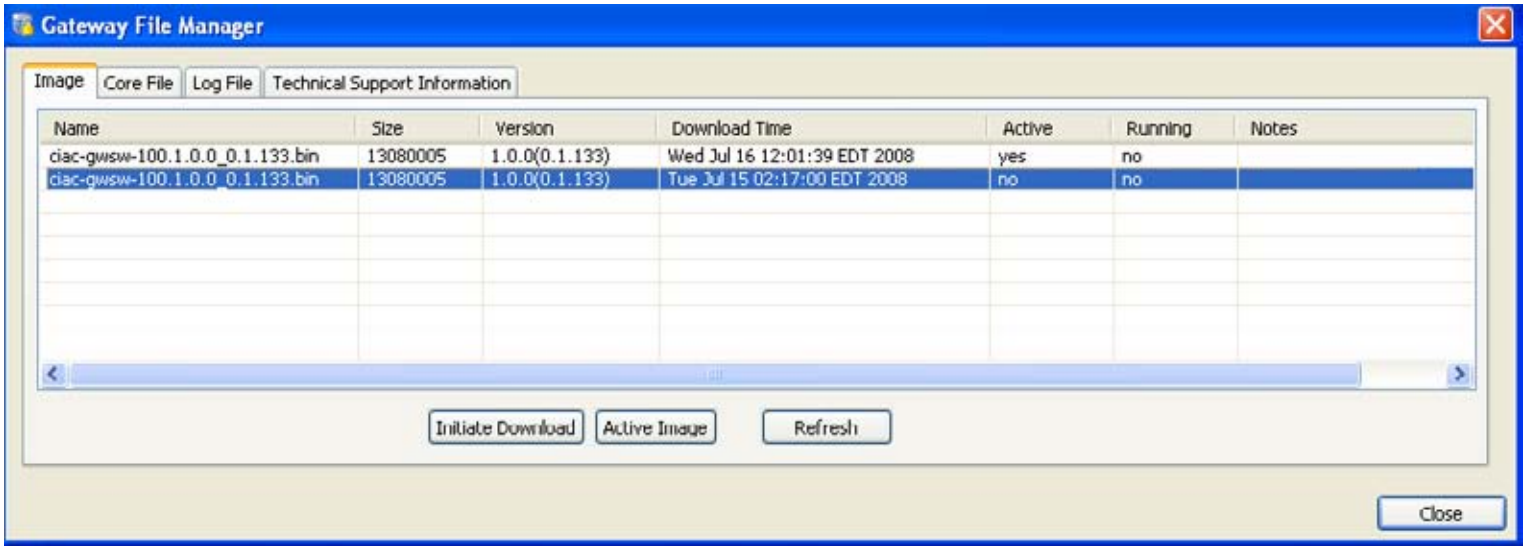
Next the Gateway File Manager is used to push the image file to the Gateway module.

Gateway keeps 2 versions of code in flash, the currently running version, and the previous version.

Next slide shows the Gateway File Manager panel.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firmware upgrade on Gateway continued



Once image is on the CPAM server, the Gateway File Manager is used to Initiate the file download, and activation.

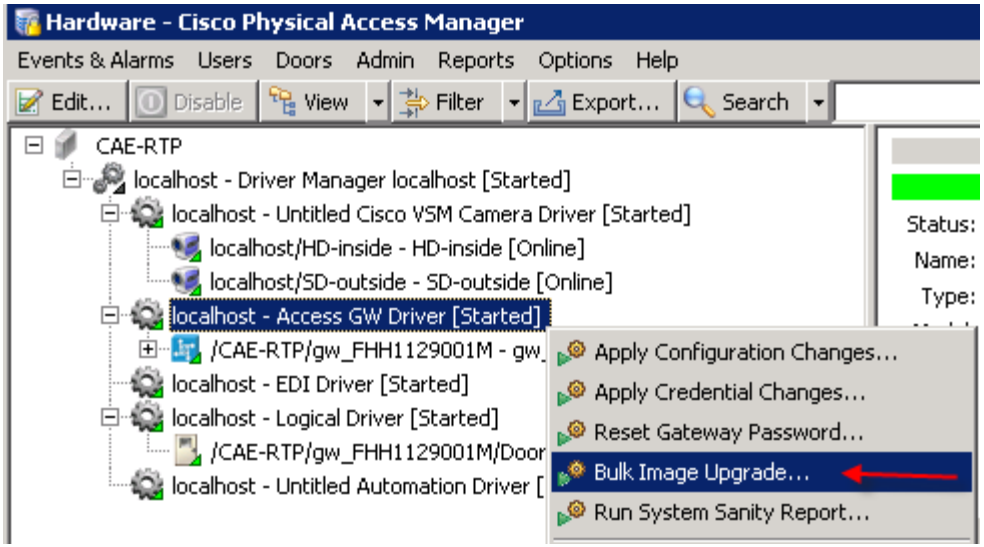
You can also use Gateway File Manager to change the active image on the Gateway from one image to the other.

There is an option to specify time of the gateway reload.

```
1.0.0(0.1.168)
      | | | build
      | | branch
      | schema
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

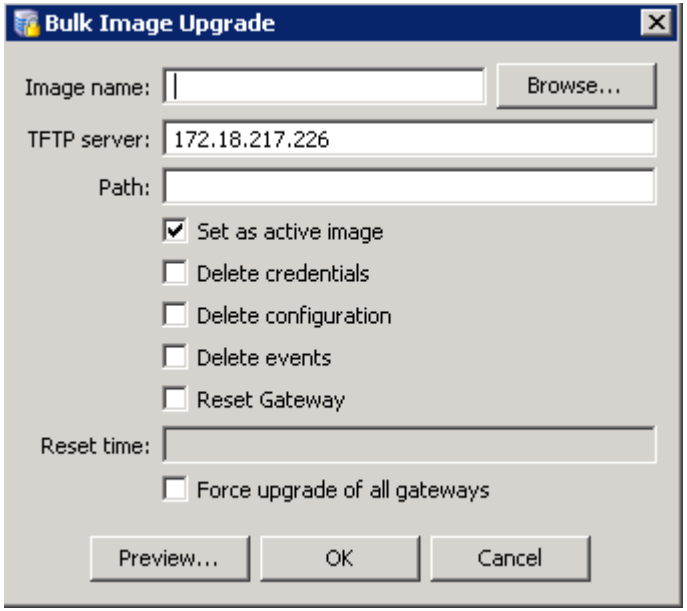
Gateway Bulk Image upgrade



Same options as seen on the Gateway Web interface for upgrades.

Performs a rolling upgrade of Gateways by upgrading 5 at a time, then moving on to the next batch.

Setting the start time of the upgrade is allowed.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

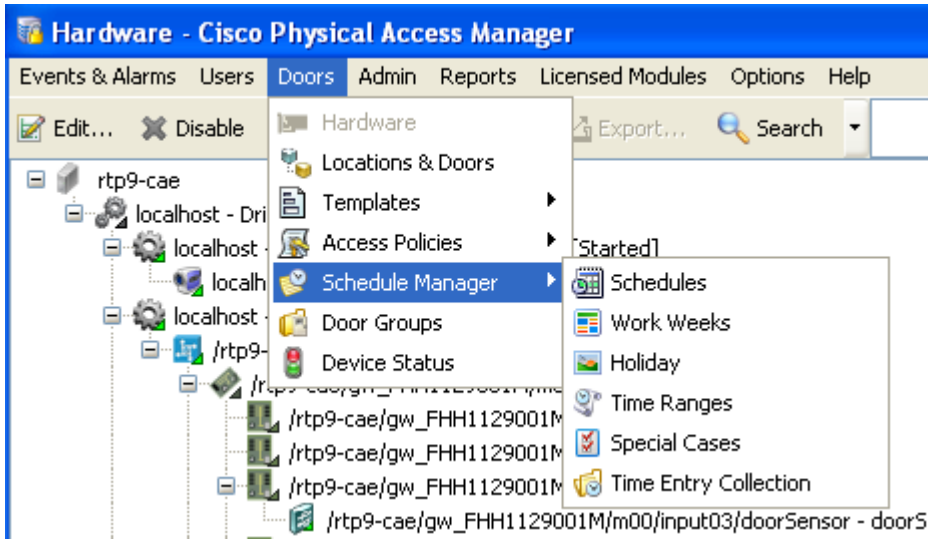
CPAM client (configuration for access)

- Schedules
- Access Policies
- Badge creation/import
- Configuration and Credential download
- Event Monitoring
- Global I/O
- Integration with VSM (Video Surveillance Manager)

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Schedules

- Schedules are created to fit the specific customer's schedule.
- Schedules are mapped to Access Policies, Door Policies, or Event Policies.



Customer can define specific schedules to meet their needs. They can define how their work weeks are laid out. Unique Time Ranges, Special cases, and Time entry collection are all managed by the Schedule Manager.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

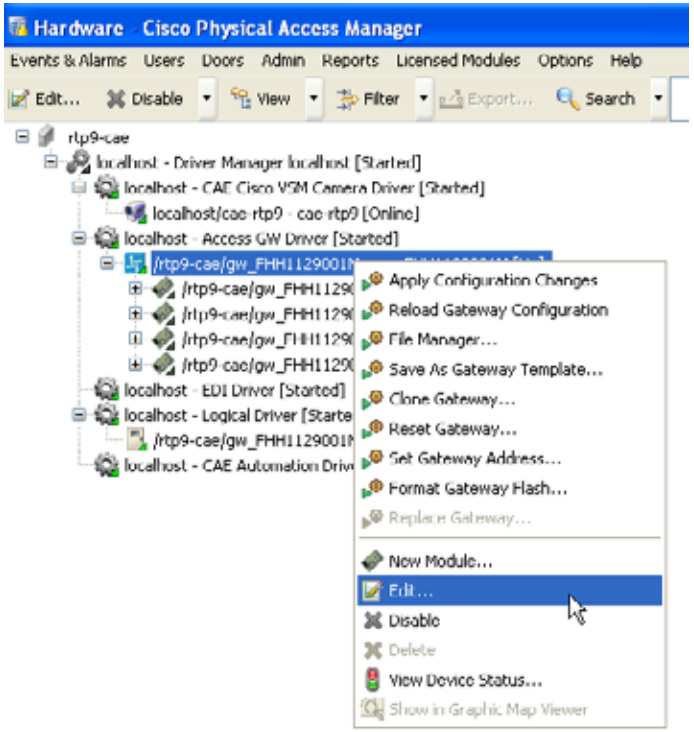
Gateway timezone

Before schedules can be accurately put in place, the Gateway time zone should be set or verified.

The Gateway clock operates on UTC and uses the time zone to determine the local time.

Time zone must be set to the time zone the Gateway is physically located in.

IE: If Gateway is in New York, and CPAM server is in Chicago, set the Gateway time zone for US/Eastern.



Can only be set via the Hardware menu, Gateway Edit, Properties

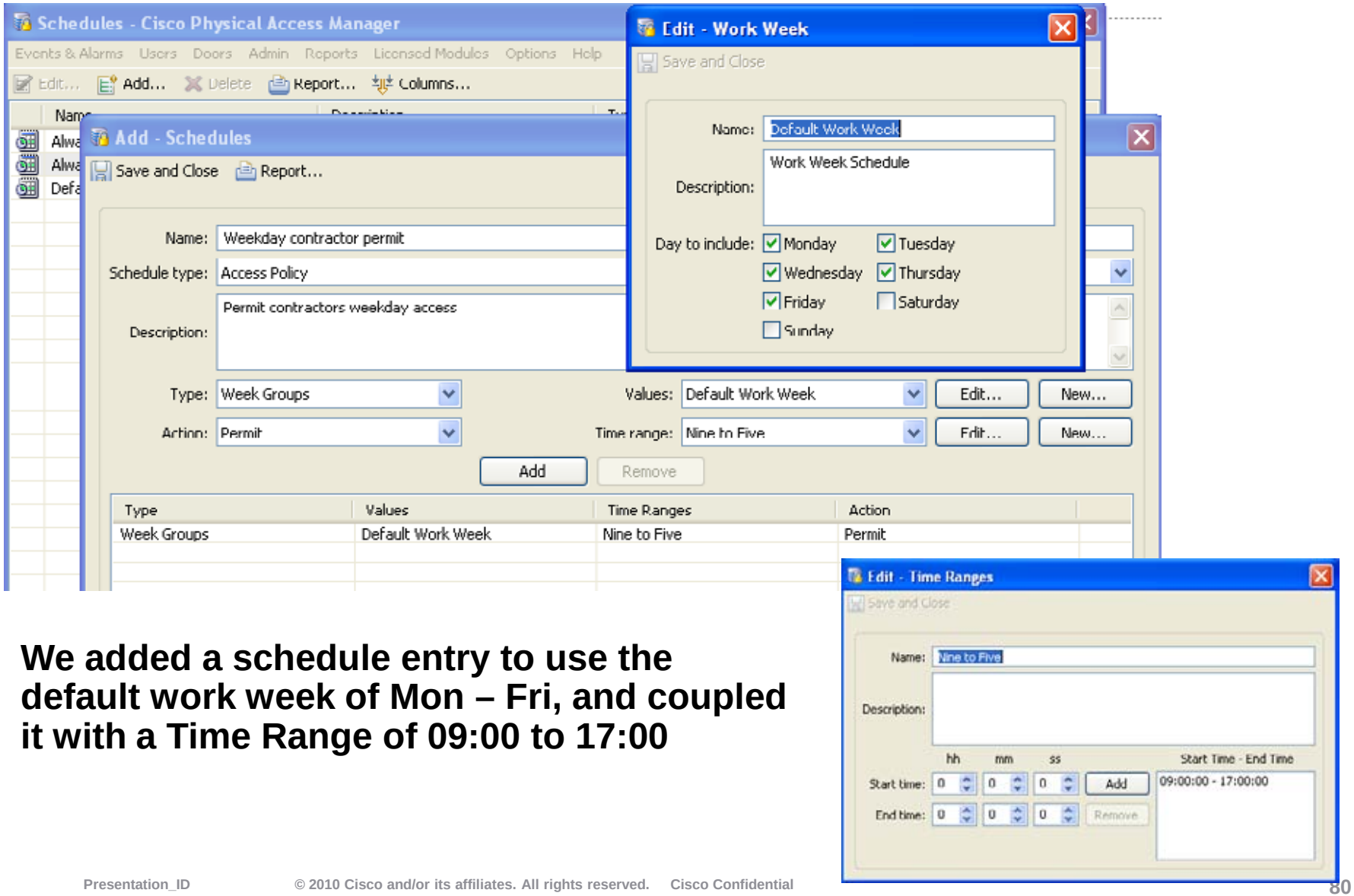
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Schedule example

- We want to create a schedule and associate it to a policy to permit ‘contractors’ badges to have access Monday to Friday, 9AM to 5PM.
- We also want these ‘contractors’ badges to be denied access on July 4th, and December 25th if those dates happen to fall on a weekday.
- Deny entries are checked first, any match = deny access.
- Permit entries are checked next, any match = grant access
- If no match is found in either Deny or Permit entries, access is denied by default.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

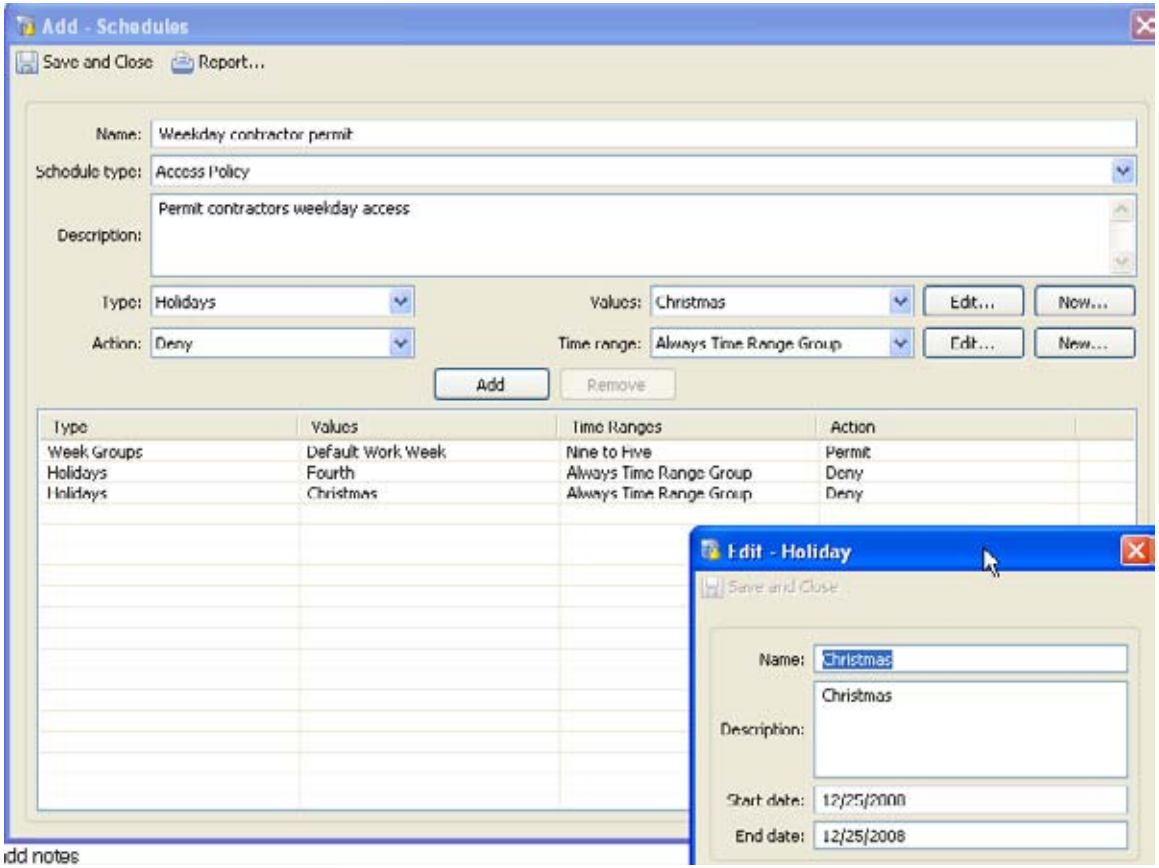
Schedule creation



We added a schedule entry to use the default work week of Mon – Fri, and coupled it with a Time Range of 09:00 to 17:00

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Deny action for desired Holidays



After adding the Permit for Mon – Fri Weekdays, we created two Deny entries. One for the 4th of July, and one for the 25th of December.

We selected Time Range of Always Time Range Group which means 00:00 to 23:59 (all 24 hours of the day we are working with)

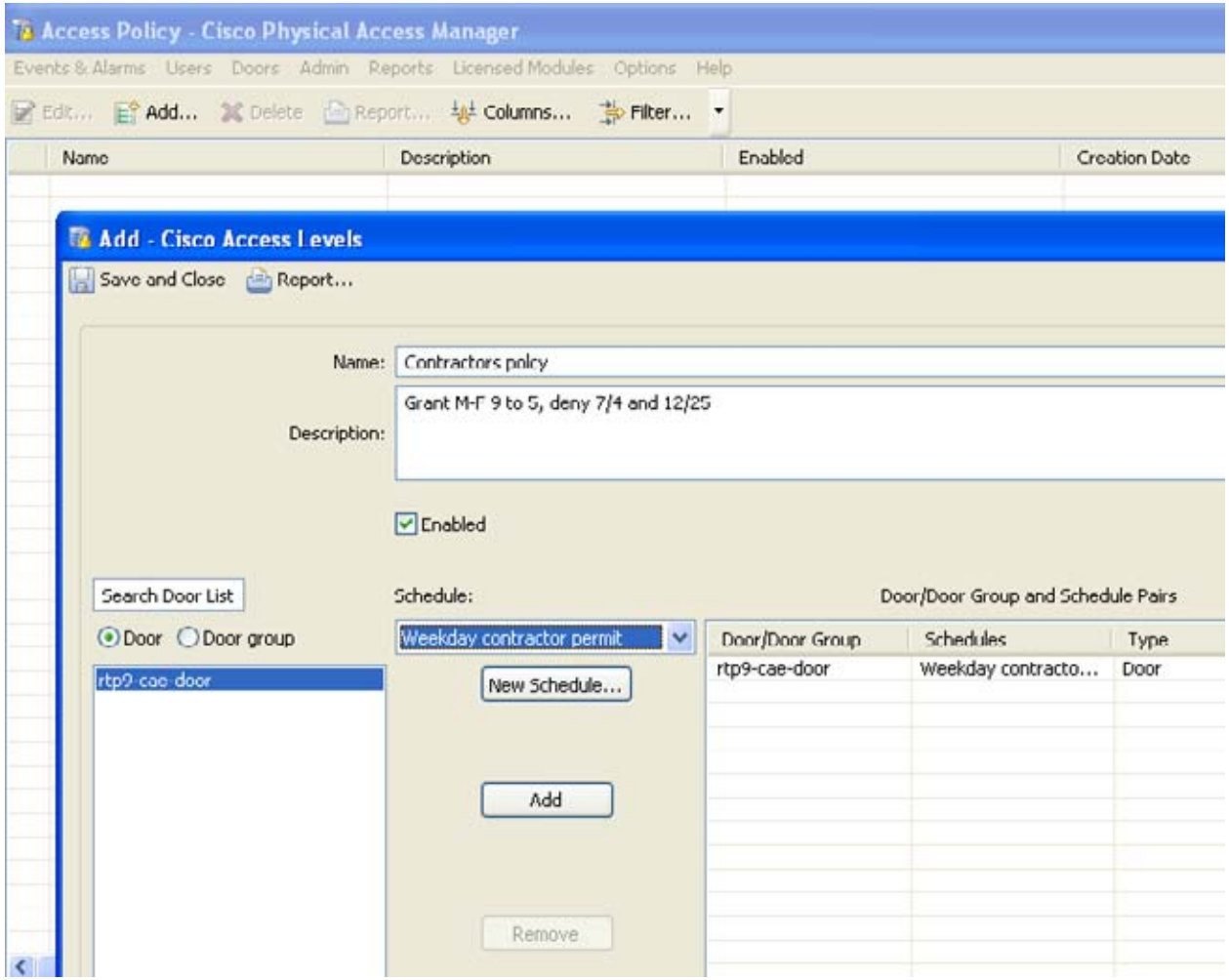
The Start and End date for the holiday for both July 4 and December 25 are the same date.

Holidays can not span between months. Create an entry for each month if needed to span a month boundary.

The schedule is now complete. Access will be granted week days from 9 to 5, and access is denied on July 4th and December 25th for this schedule. Next step is to associate this schedule with an Access Policy.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Policy creation



Here we created a Policy and added the description.

We associated the Door with the schedule and created the policy.

Door Group can be used to associate multiple doors to a policy.

Example, we could have created a door group that included all perimeter access door, and applied this policy to the door group as opposed to having to apply the policy to each perimeter door individually.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configuring a badge for access

Accessed from main menu.

Can Add, Edit, or Disable badges.

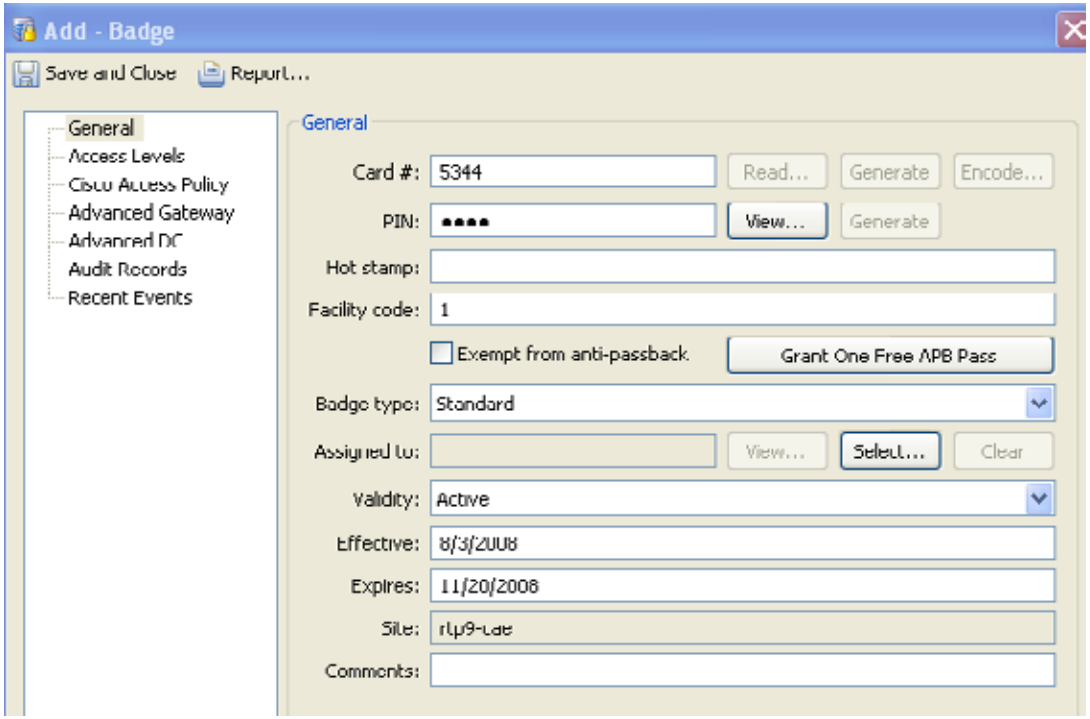
For audit reasons badges are never deleted, only disabled.

Card number is imbedded in the card.

PIN is required even if not used, can be disabled globally.

Facility code is imbedded in card, decisions can be made based on this code.

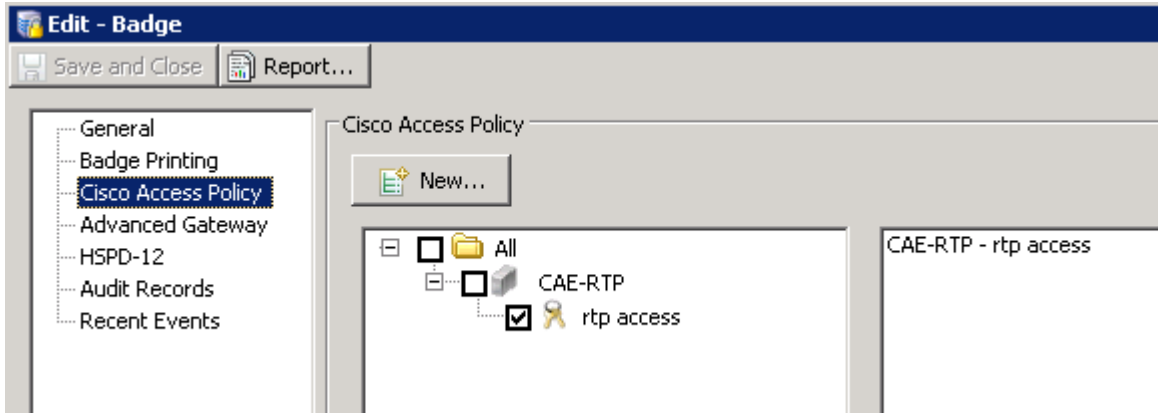
If not entered, Effective and Expires dates are not used and badge is valid from today until it is manually changed.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Badge Access Level and Policy

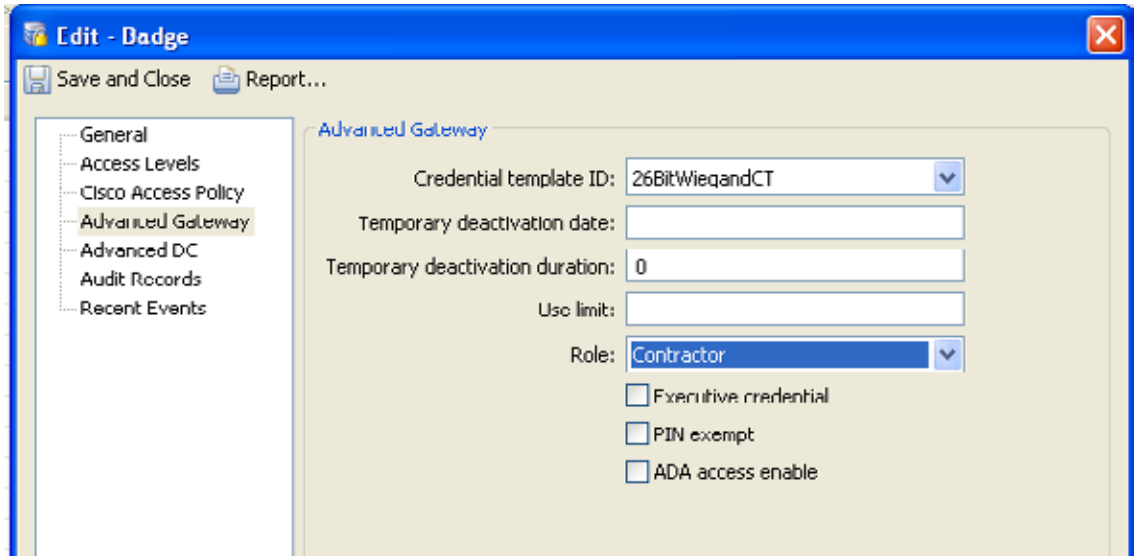
Cisco Access Policy is what is used to tie badges, to time/date and door access.



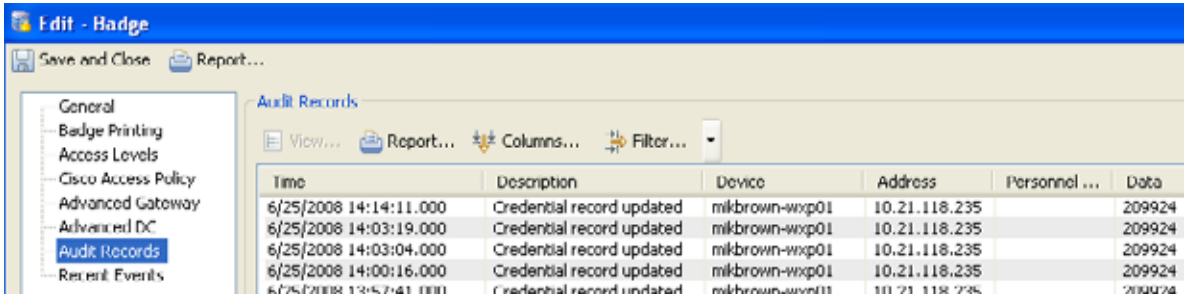
Which location and what access policy will this badge adhere too?

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Badges continued



Audit records for available for badge record edits



Credential template must be associated to the badge.

Temporary deactivation can be configured for the badge.

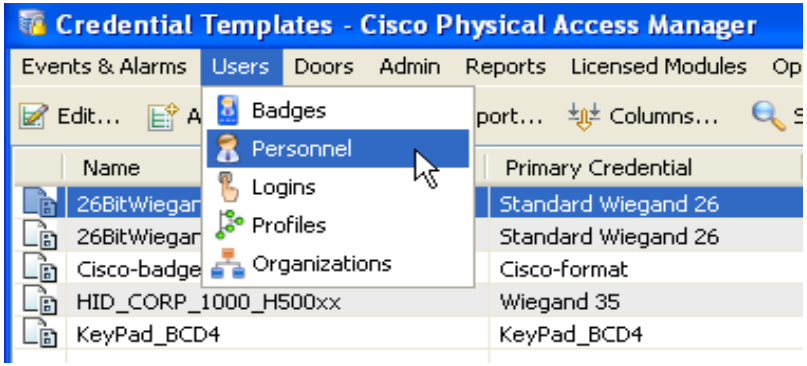
Role must be assigned.

Badge can be exempt from need to also enter PIN when readers at facility include keypads.

ADA access mode can be assigned to the badge. This would provide longer access time for disabled persons when passing through a door.

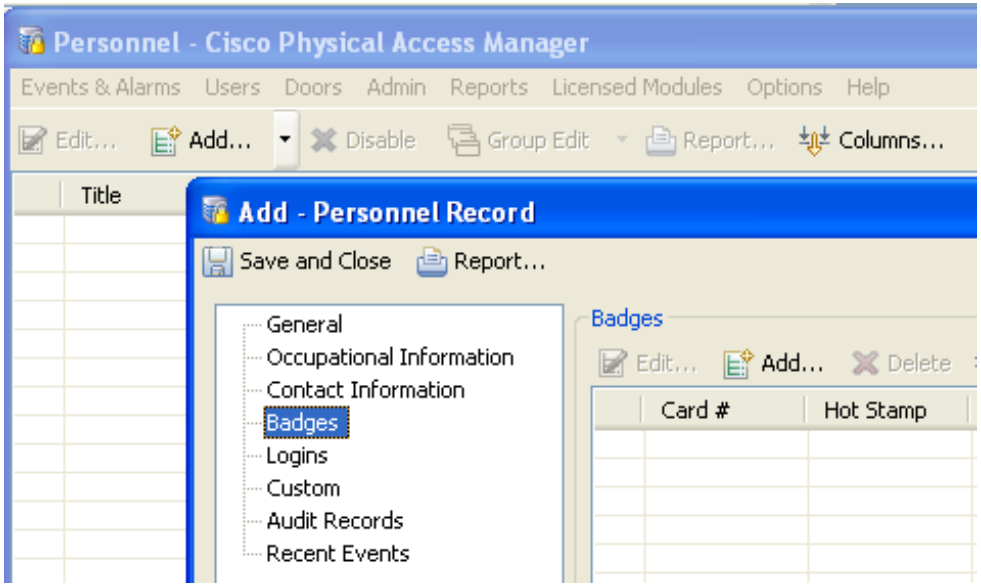
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Badges are then associated to people



Personnel records are created or edited to add in the badge, or badge numbers associated to that person.

It is possible for a person to have multiple badges associated to them.

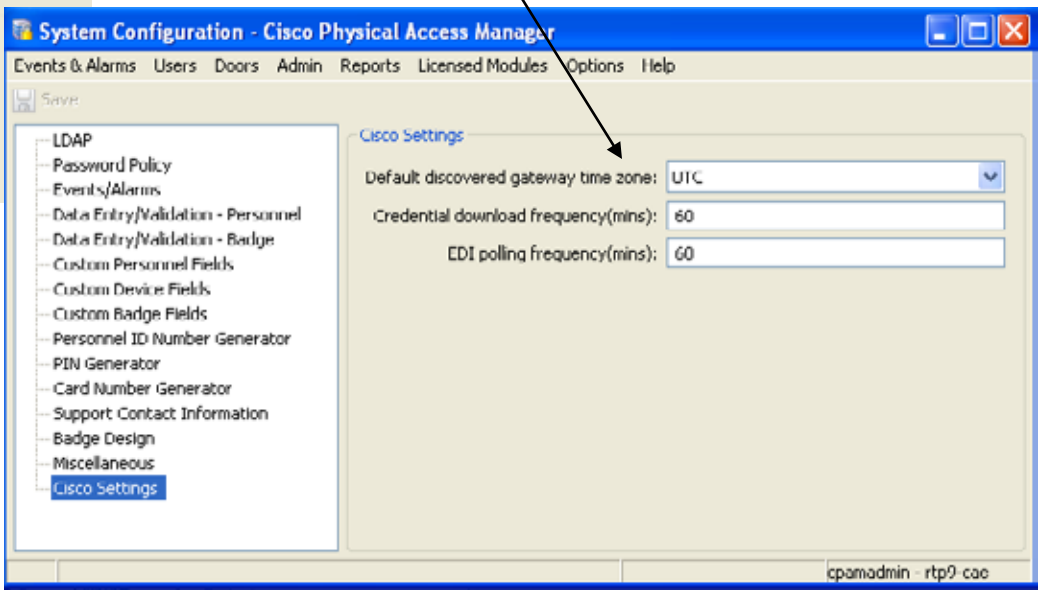


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Credential download

- Credential database is synced between the CPAM server and the Gateways every 60 minutes by default.
- This interval is configurable under System Settings

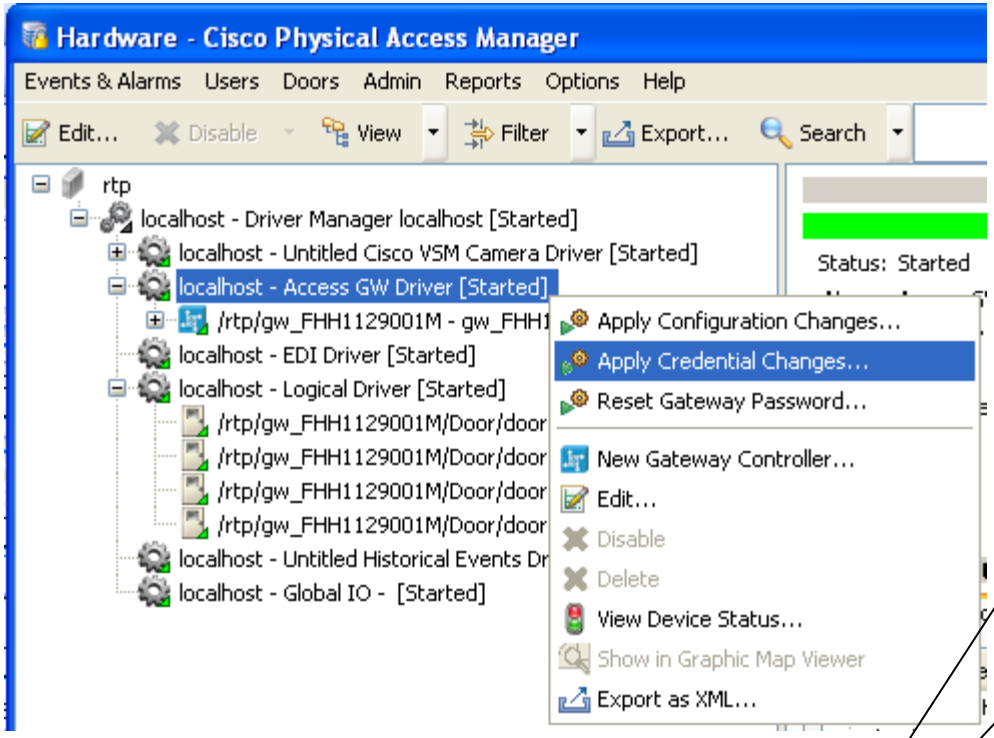
Default Gateway time zone is also set under System Configuration



Changing the download interval requires CPAM application to be stopped and re-started to make changes effective

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Manual download of credentials

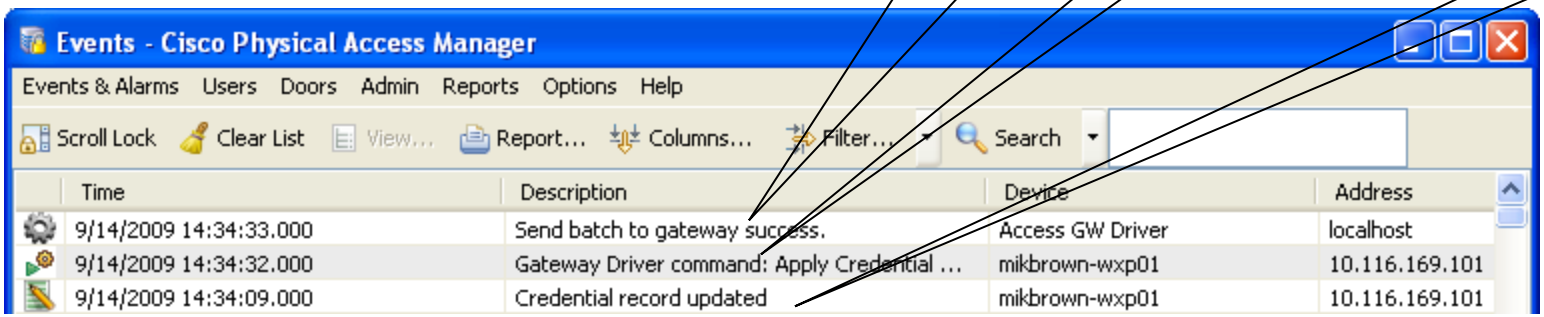


If you update a badge credential and want to manually push the change to the Gateways, right click on the Gateway Driver, and then left click on Apply Credential Changes.

This message means the update was sent to the Gateway. Should see this message for each Gateway

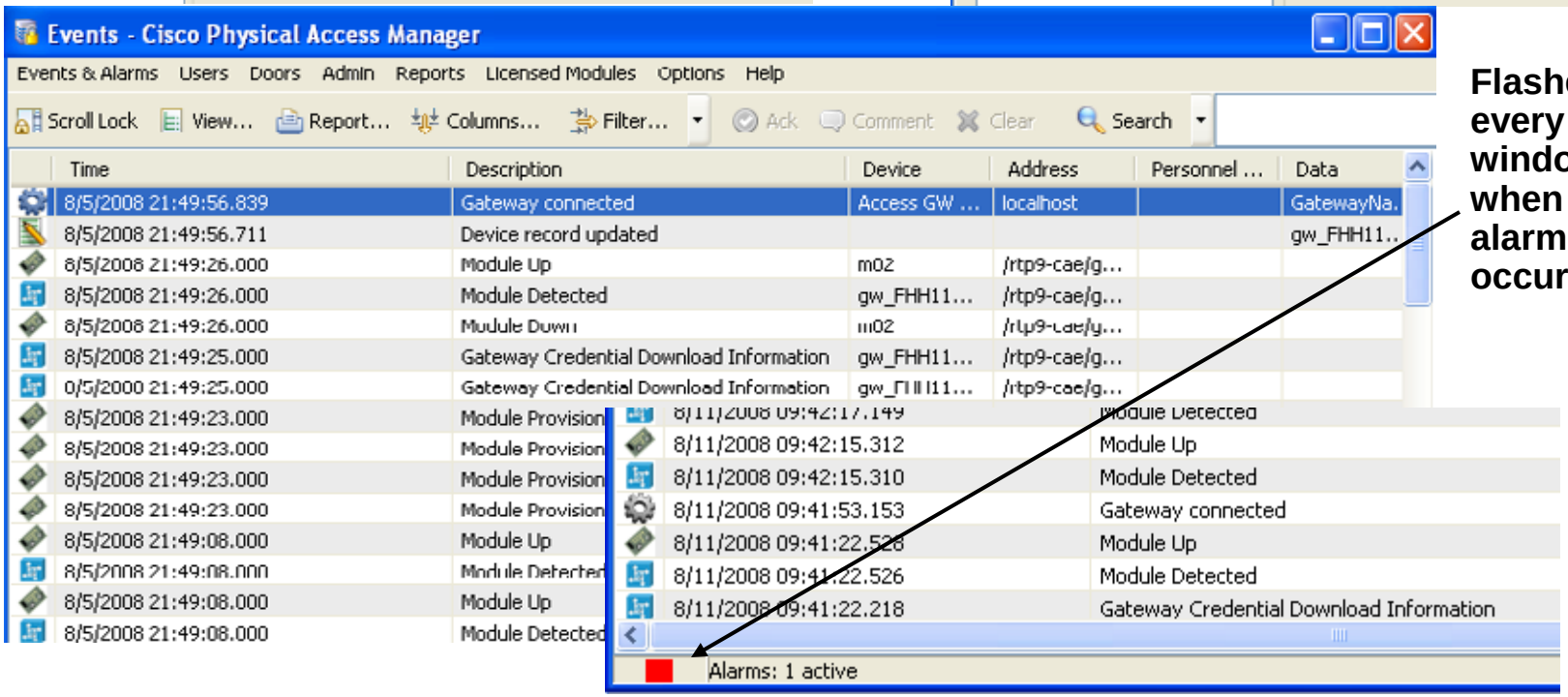
Credential changes applied manually

Badge record is updated.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Event Monitoring



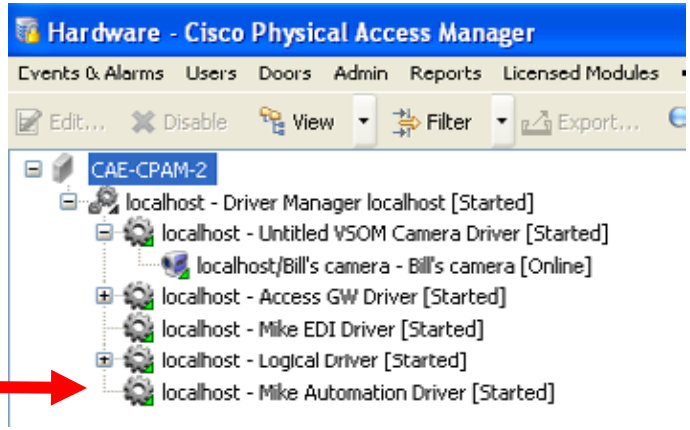
Flashes on every window when alarm occurs

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

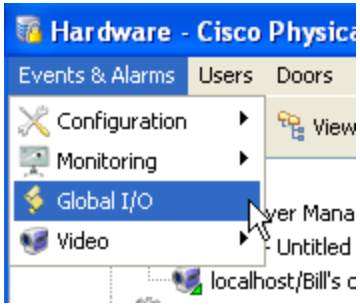
Global I/O to take action on a trigger

- Automation driver must be started
- Used to trigger some action
- Examples:

Turn on light or send email



Next we go to the Global I/O menu and define what the trigger event is, and what action to take on the event.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Global I/O

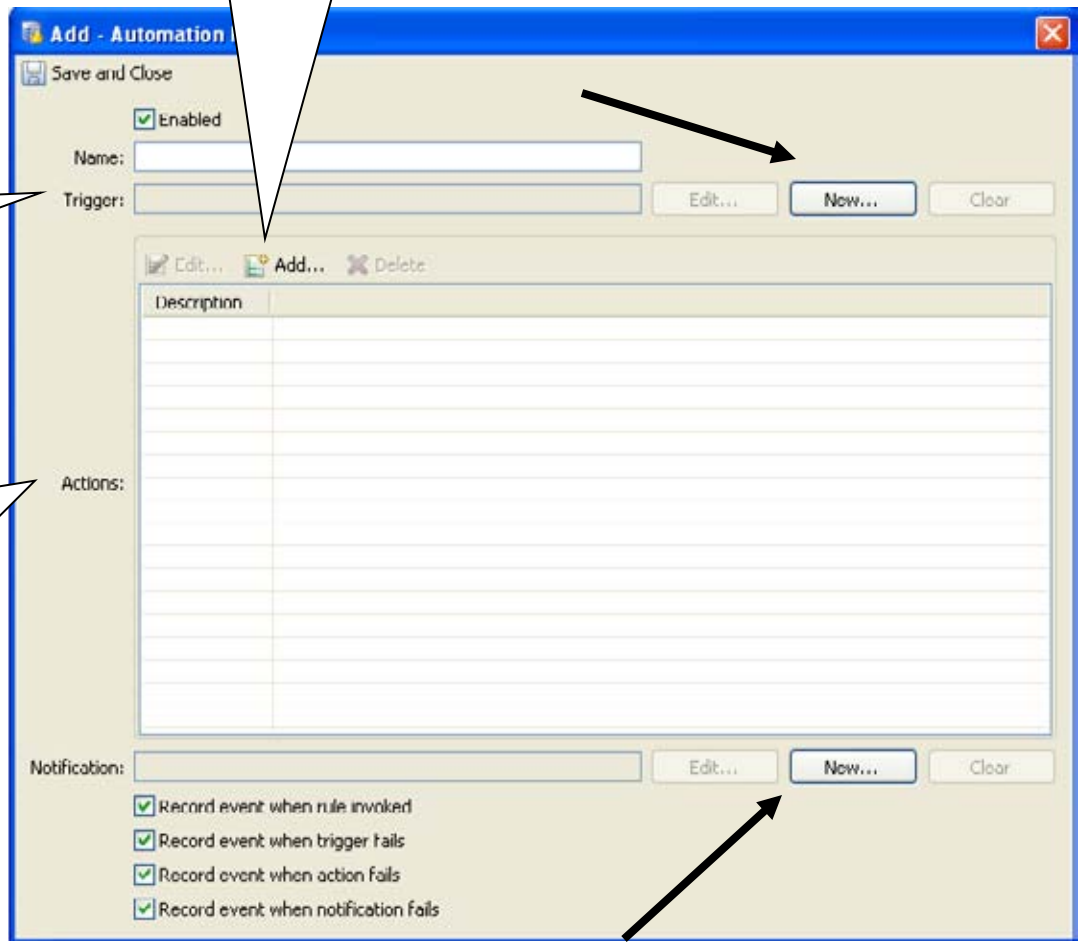
Add option is used to allow multiple actions on a single trigger

External triggers can be wired and configured as inputs as required.

Event trigger is defined, this can based on any event or message posted in the log.

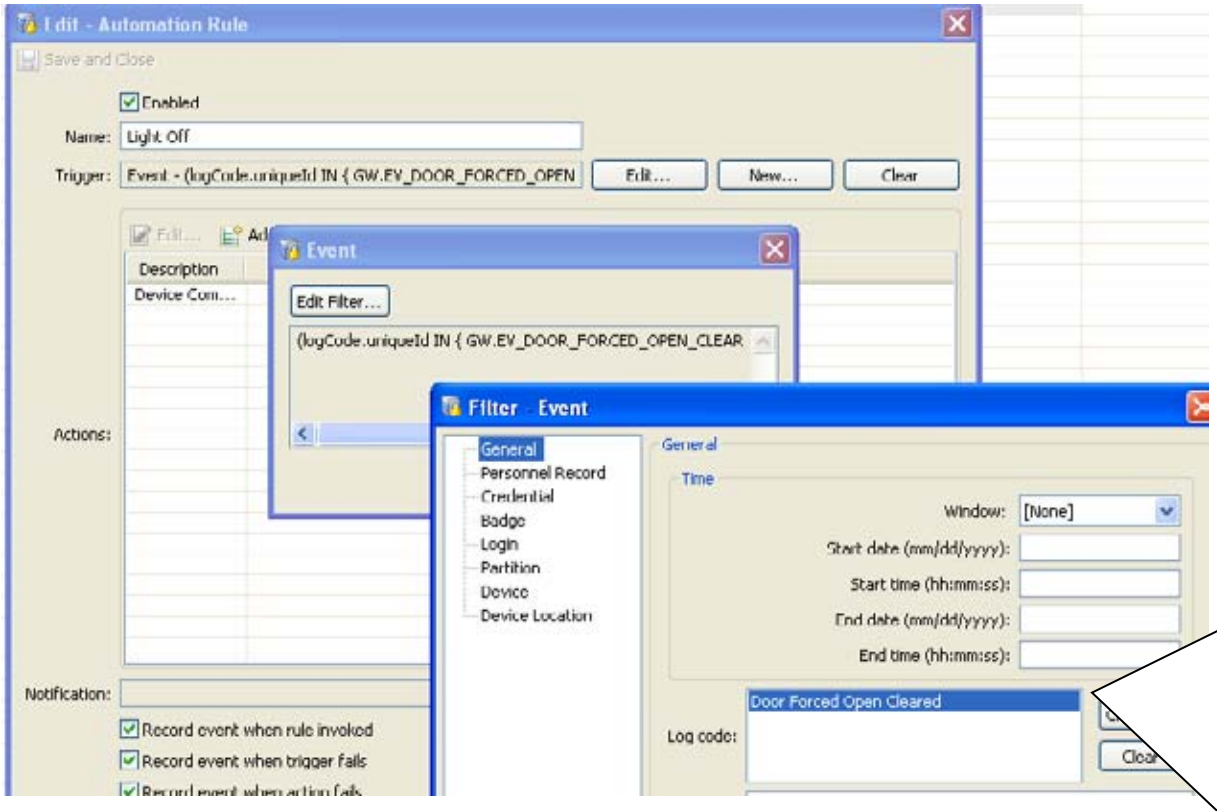
Actions to perform are defined. The action can be to perform a specific command a specific device. IE: close the relay for module 3, output 2 to turn on a light.

Also can generate a notification email.



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The trigger



Here we have the ability to use any event message logged as the trigger event.

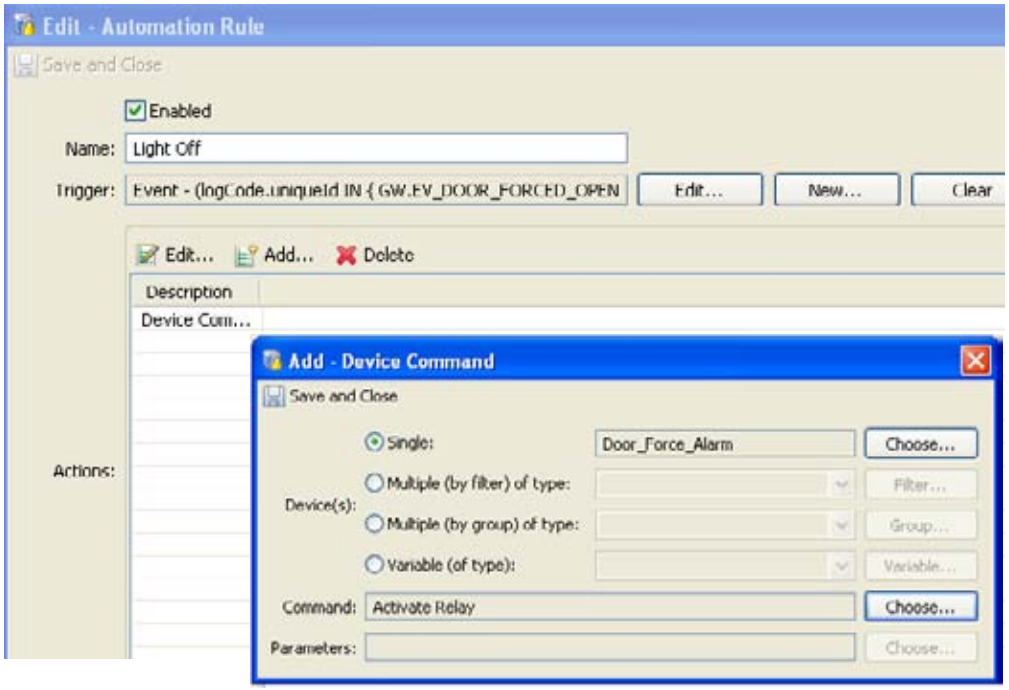
In this instance, we are using the Door Forced Open Cleared message as our trigger.

We did not specify a specific door, so this message for any door will be considered a trigger.

<u>Choose</u> provides a menu to select a specific message from the logged events.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The action

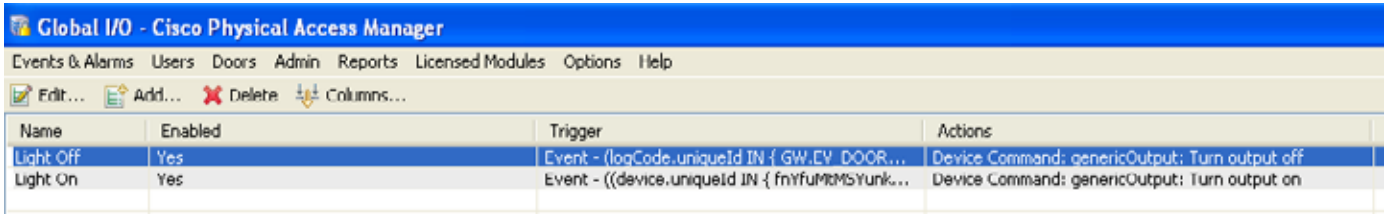


Under Action, we added a Device Command.

We then selected the specific device we want to take action on from the hardware tree.

In this example, we are using a generic output to turn off a light if the trigger event occurs.

We use the Command and Choose to select the action to be performed.



Here we used a trigger of ‘Door Forced Open’ to turn on a light, and a second trigger of ‘Door Forced Open Cleared’ to turn the light off.

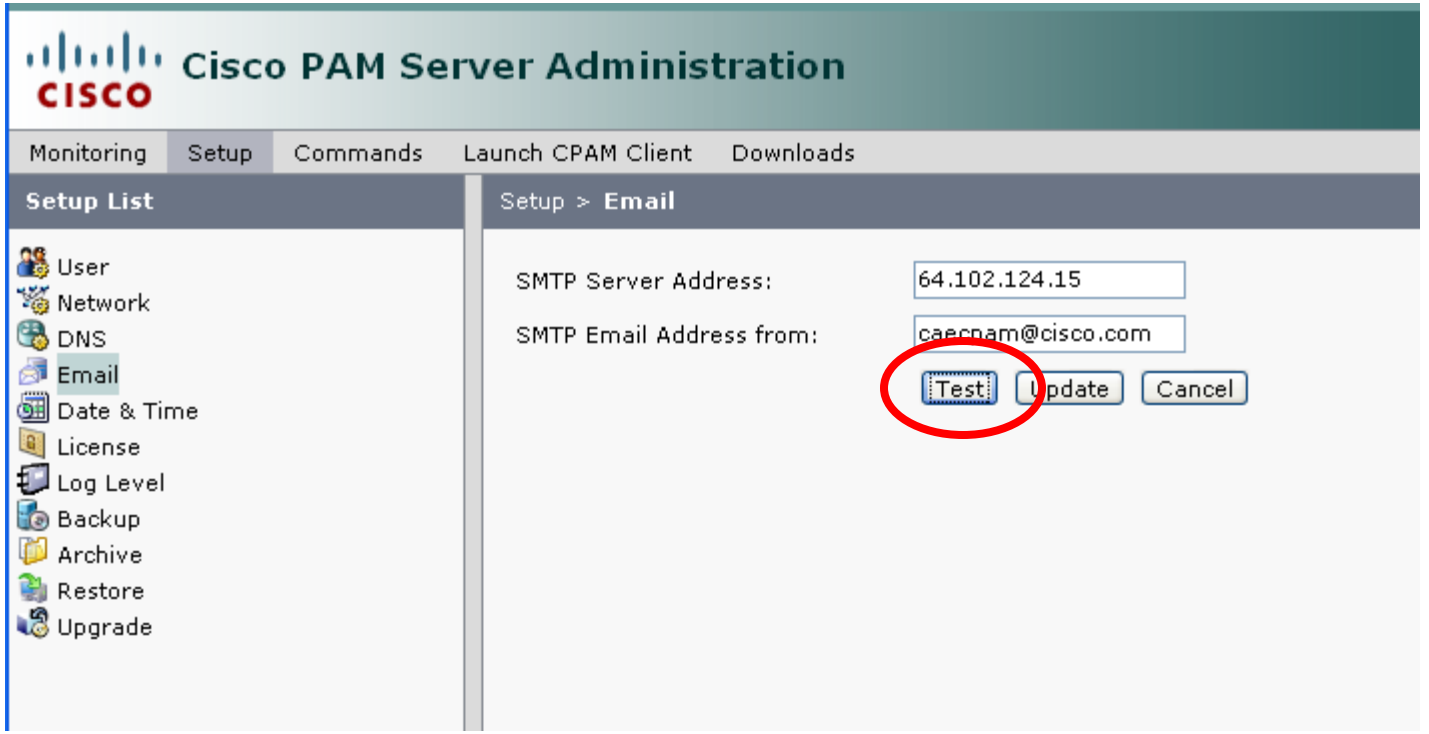
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Email notification TEST

You can use the CPAM web interface to test the SMTP options.

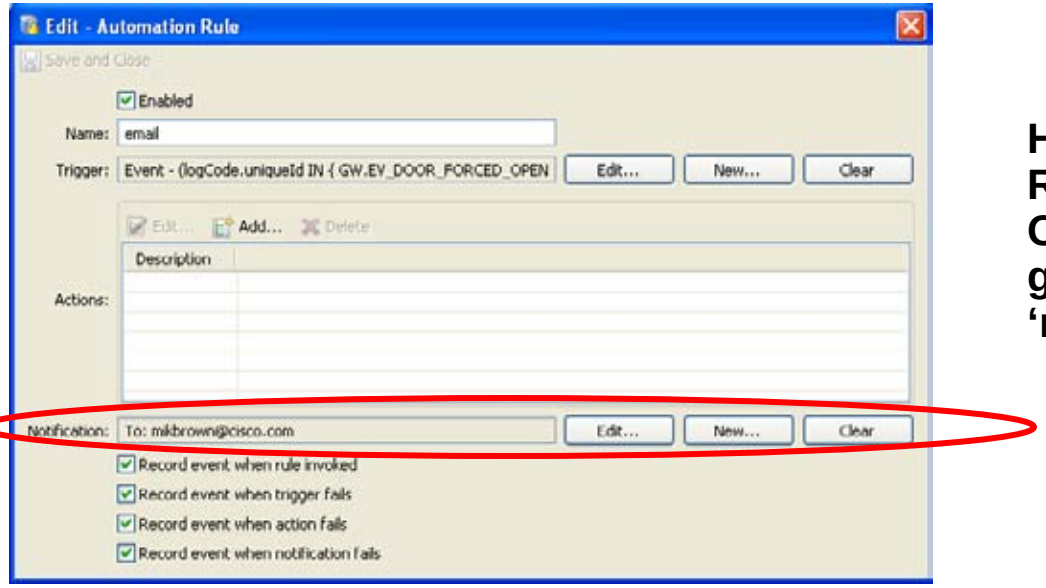
The Test option is located under the Setup menu, Email item.

Configuration here will not be used for the Automation Driver to send email notifications.

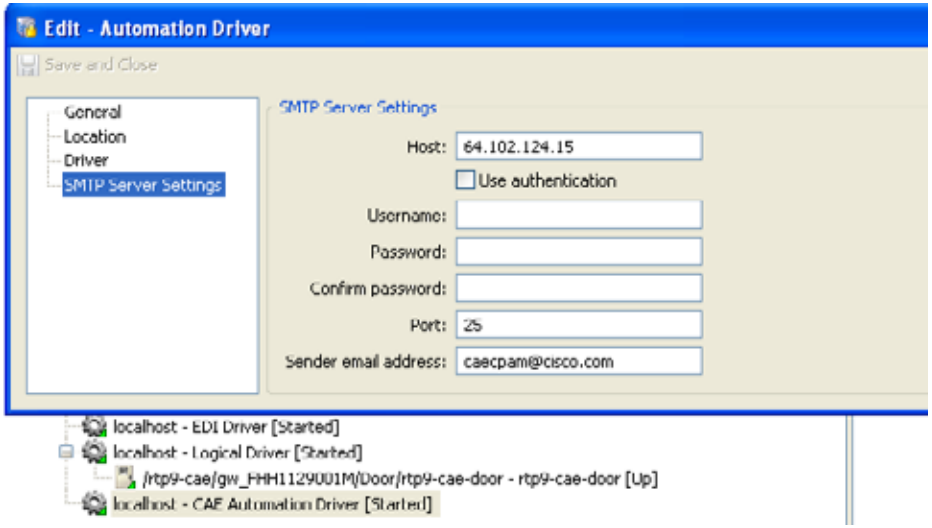


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Email notification for events



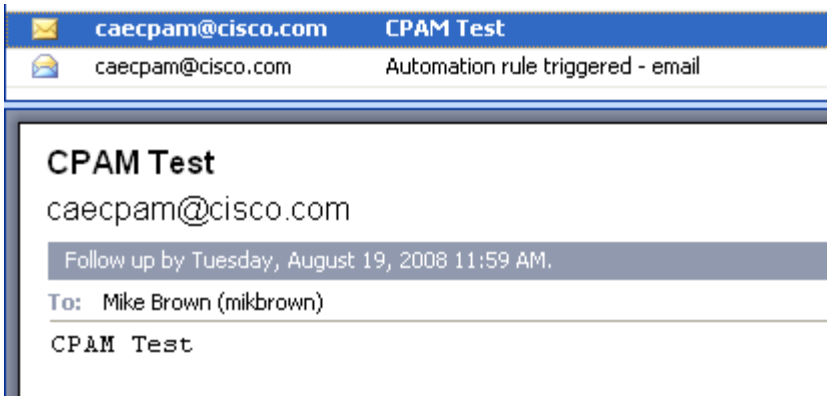
Here we see and Automation Rule that uses 'Door Forced Open' message/event to generate an email to 'mikbrown@cisco.com'



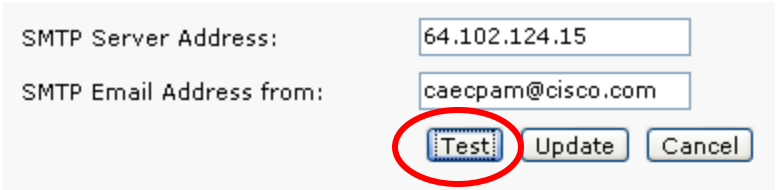
Automation driver must be configured with SMTP settings before the Notification email can be sent from the CPAM server. The driver must be restarted once the SMTP server settings are configured.

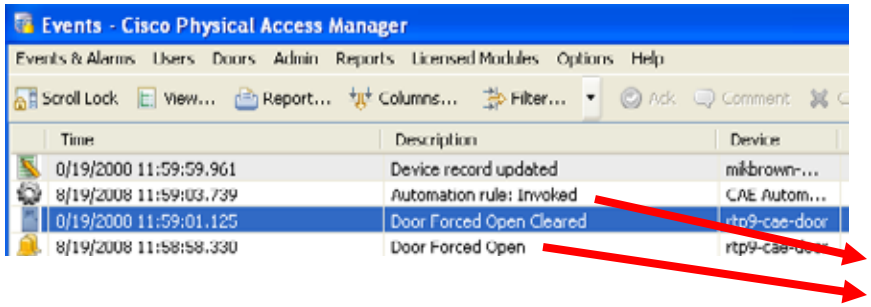
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sample email text

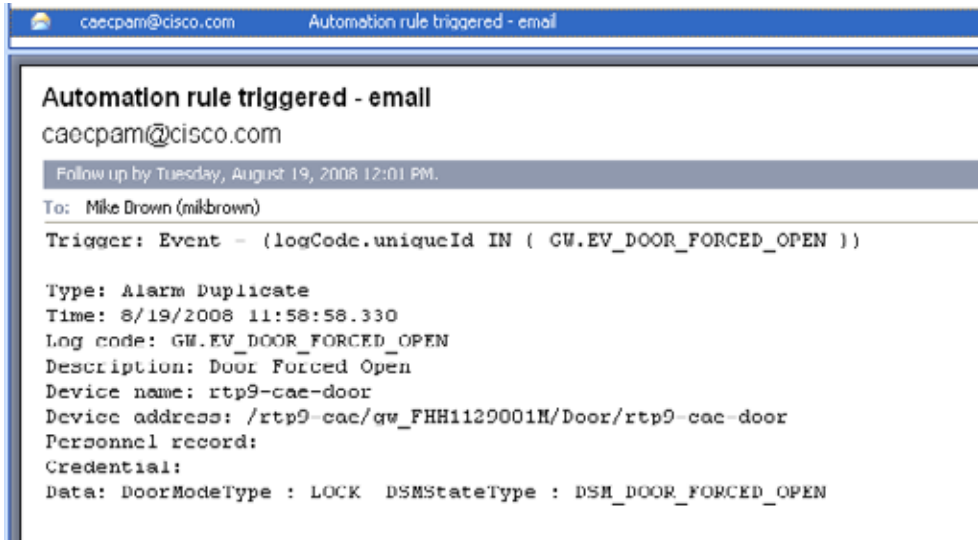


Test email generated by the CPAM server Test option





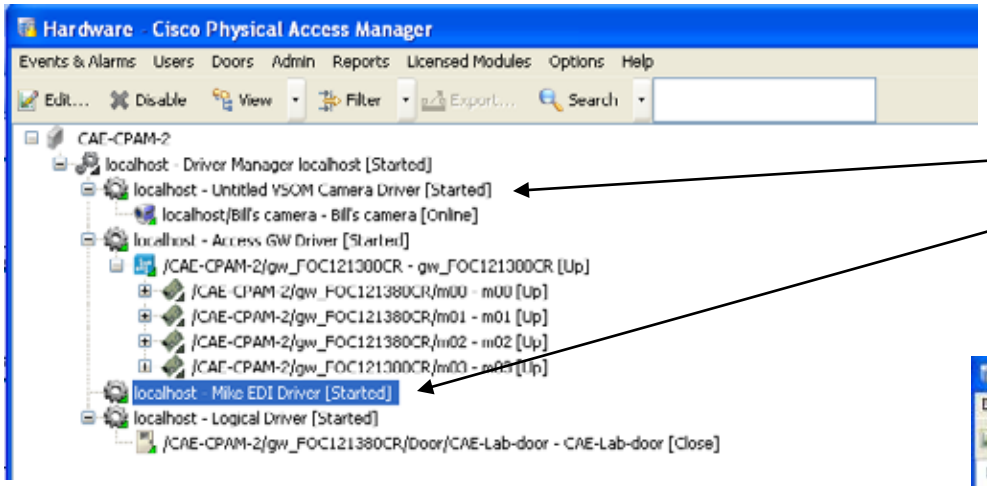
Email generated by the Automation Driver triggered by the Door Forced Open event.



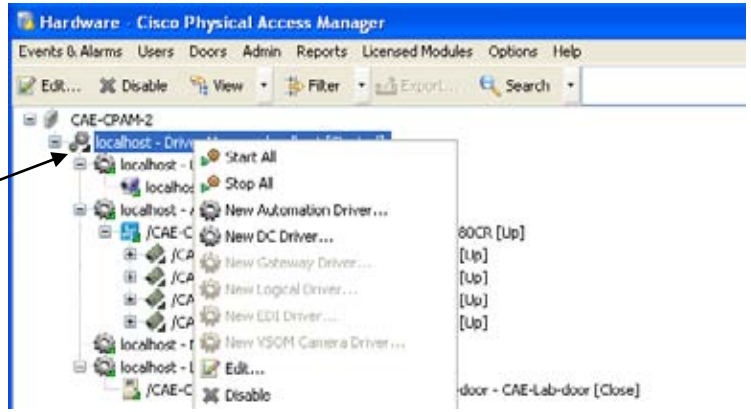
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video Integration

- EDI driver will start automatically, user must manually start the VSOM Camera Driver. EDI and VSOM Camera Driver should both be running.


Hardware - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Licensed Modules Options Help
Edit... Disable View Filter Export... Search
CAE-CPAM-2
localhost - Driver Manager localhost [Started]
localhost - Untitled VSOM Camera Driver [Started]
localhost/Bill's camera - Bill's camera [Online]
localhost - Access GW Driver [Started]
/CAE-CPAM-2/gw_FOC121300CR - gw_FOC121300CR [Up]
/CAE-CPAM-2/gw_FOC121380CR/m00 - m00 [Up]
/CAE-CPAM-2/gw_FOC121380CR/m01 - m01 [Up]
/CAE-CPAM-2/gw_FOC121380CR/m02 - m02 [Up]
/CAE-CPAM-2/gw_FOC121380CR/m03 - m03 [Up]
localhost - Mike EDI Driver [Started]
localhost - Logical Driver [Started]
/CAE-CPAM-2/gw_FOC121380CR/Door/CAE-Lab-door - CAE-Lab-door [Close]

Check for both to show Started status.

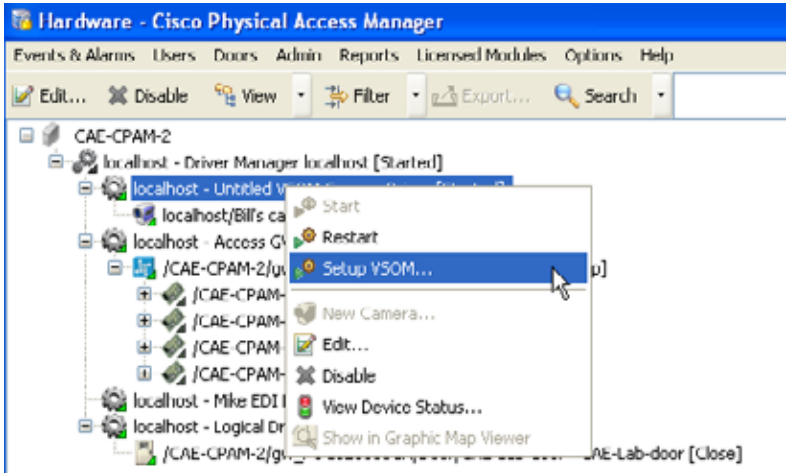


If they are missing, or Stopped, Right click on the Gateway, and then in the drop down start, or create new driver.

You can only start 1 instance of each. If it is already created, the New driver is grayed out.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

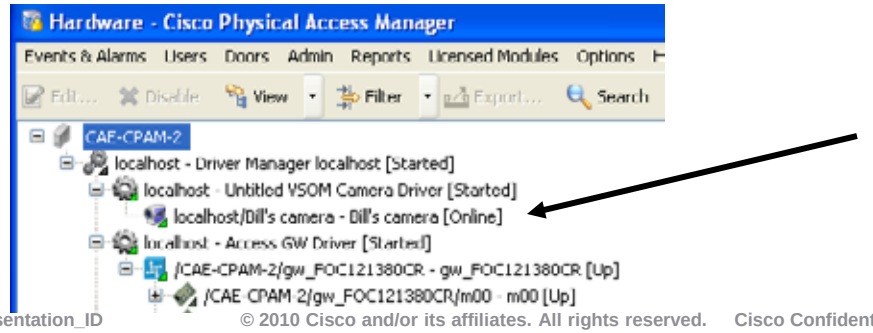
Camera associations

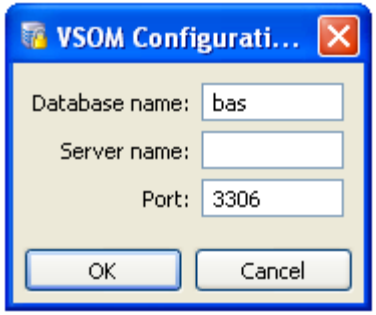


Once the drivers are started, you need to point to the VSOM server so CPAM can obtain the camera list. Right click on the VSOM driver to get to the Setup VSOM menu.

You enter the IP address, or the DNS name of the VSOM server. If this works, the Cameras should be displayed under the VSOM driver

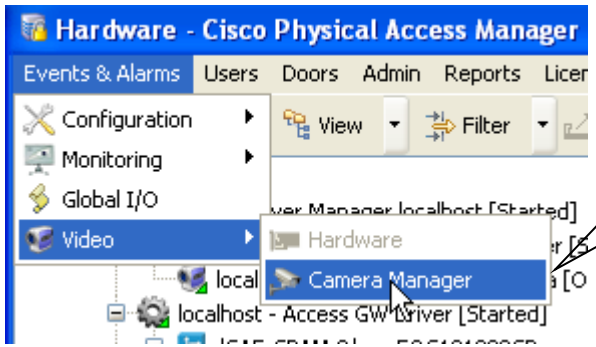
bas is the default database name in the VSOM server, and 3306 is the default port for MYSQL.


Hardware - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Licensed Modules Options
Edit... Disable View Filter Export... Search
CAE-CPAM-2
localhost - Driver Manager localhost [Started]
localhost - Untitled VSOM Camera Driver [Started]
localhost/Bill's camera - Bill's camera [Online]
localhost - Access GW Driver [Started]
/CAE-CPAM-2/gw_FOC121380CR - gw_FOC121380CR [Up]
/CAE-CPAM-2/gw_FOC121380CR/m00 - m00 [Up]

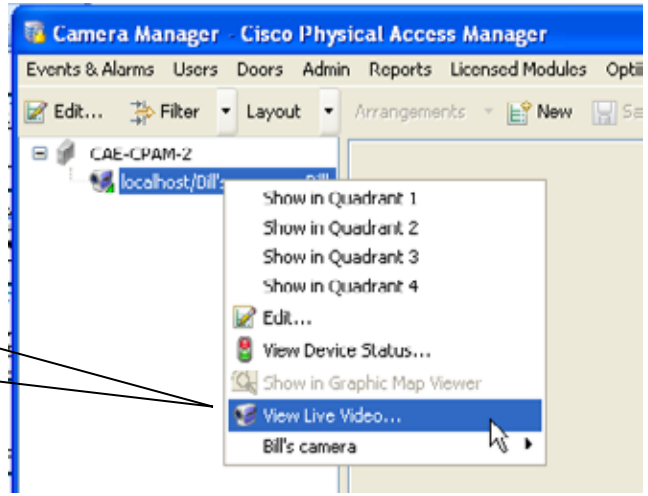


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

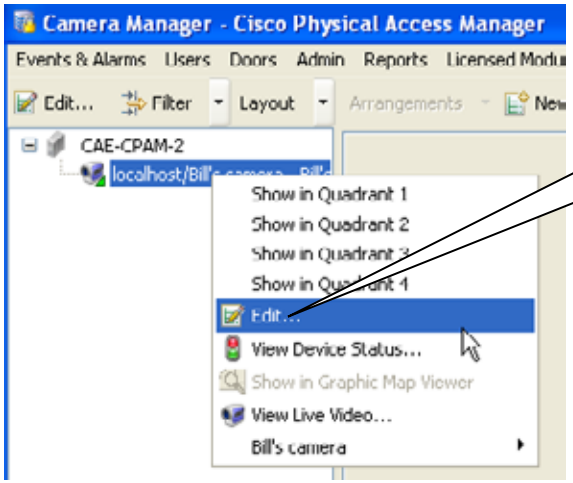
Camera Manager and door associations



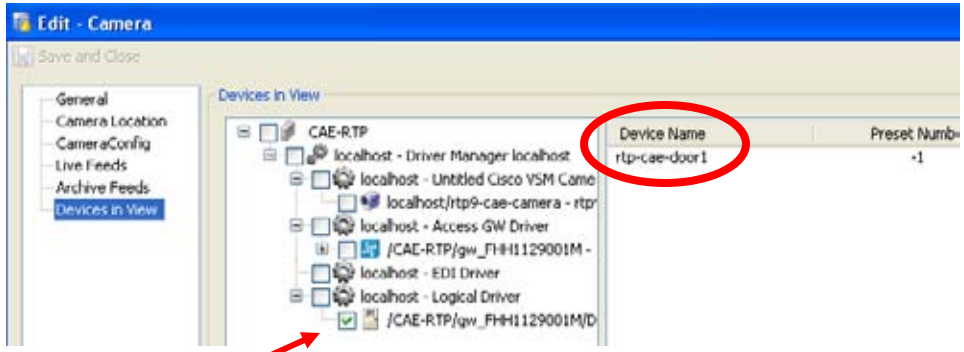
Camera Manager is under Events & Alarms



Check the Live Video feed to validate that the camera is functioning



Edit the Camera to associate it with a Door

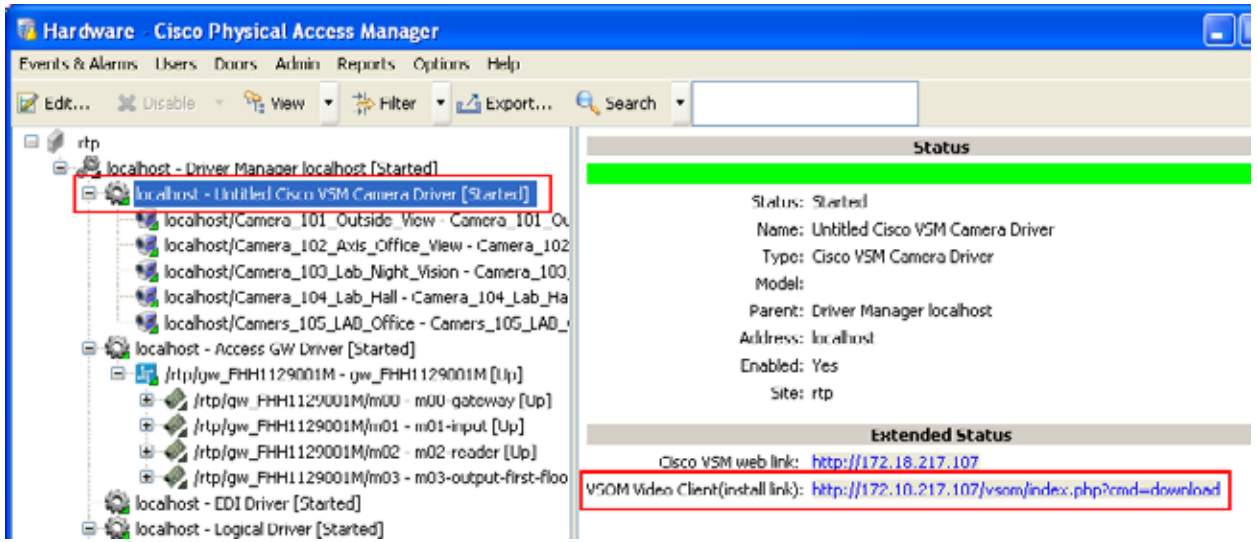


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Alarms and video

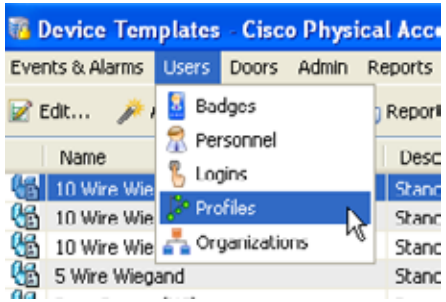
- Once camera and door are associated, any Alarm event at the door can generate a video popup window showing the camera feed. This depends on the user profile.
- By default, a max of 4 video feeds will be automatically popped up on the client screen so that client PC resources (memory) are not exhausted.
- Video Player must be downloaded separately from the VSOM server.

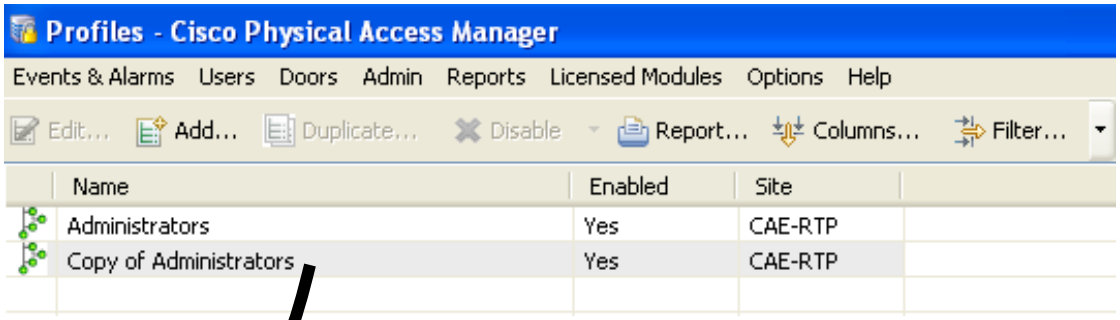
For PTZ cameras, you use the presets from VSOM to populate the preset field in the camera configuration in CPAM.

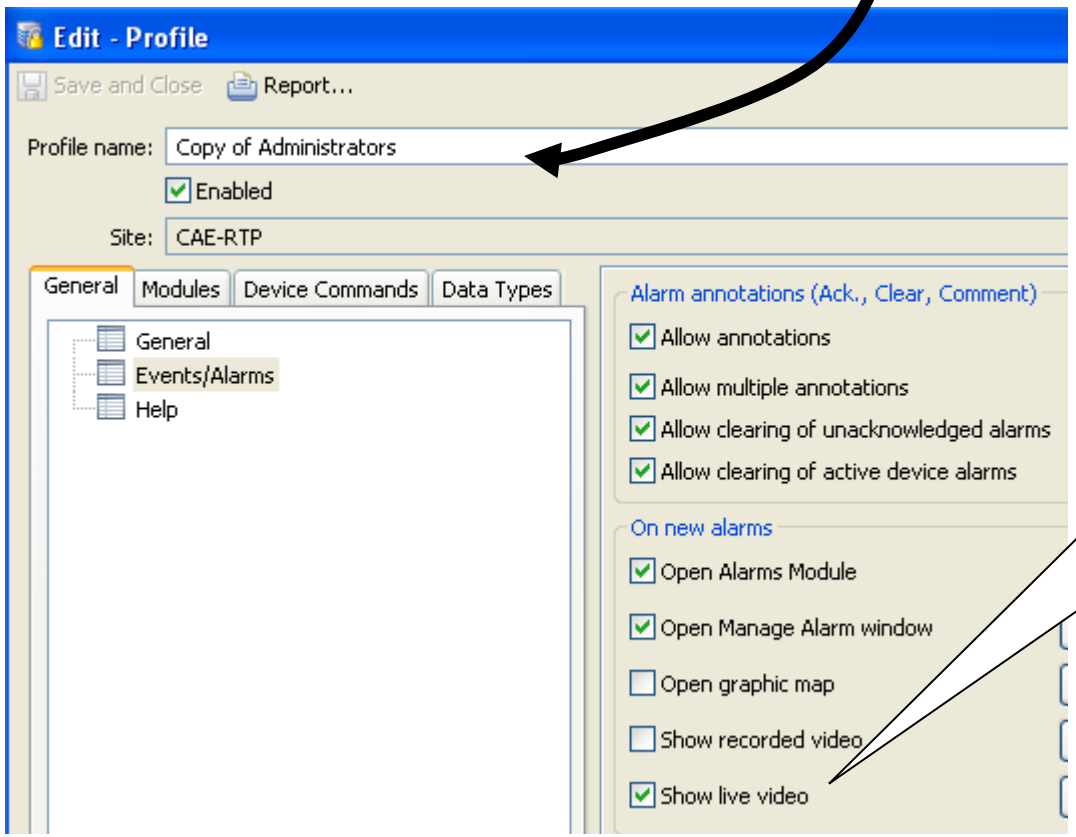


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

User profile must be configured to show video





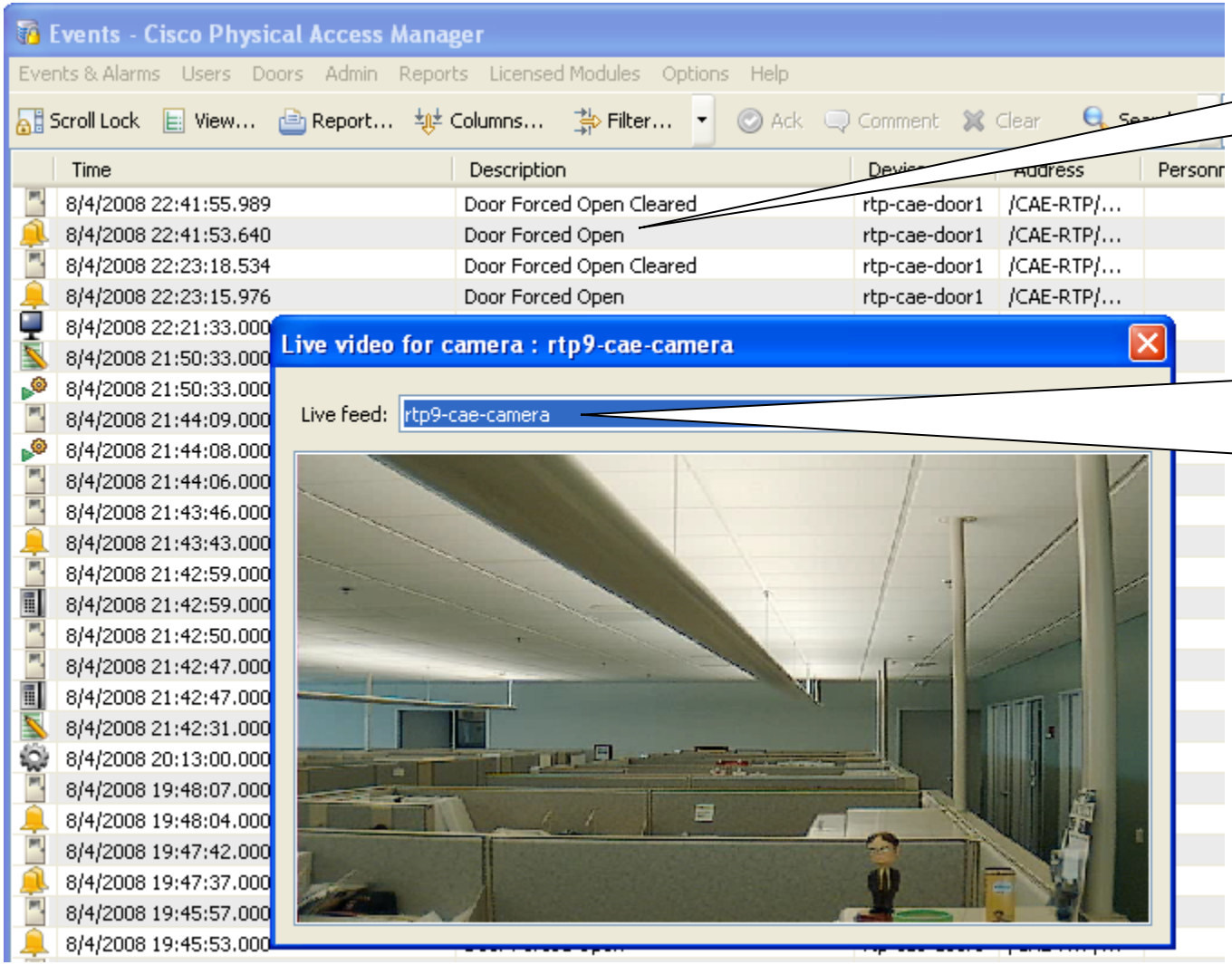


CPAM user profile must be set to allow pop up video window.

The default Administrators profile has this box unchecked, and it can not be checked

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Alarm can trigger live video popup



Alarm caused by Door Forced Open event.

Camera feed associated to the door is automatically opened and displayed for the operator

This opens a TCP connection from client machine to the VSOM server and the video is streamed over the TCP connection using port 80.

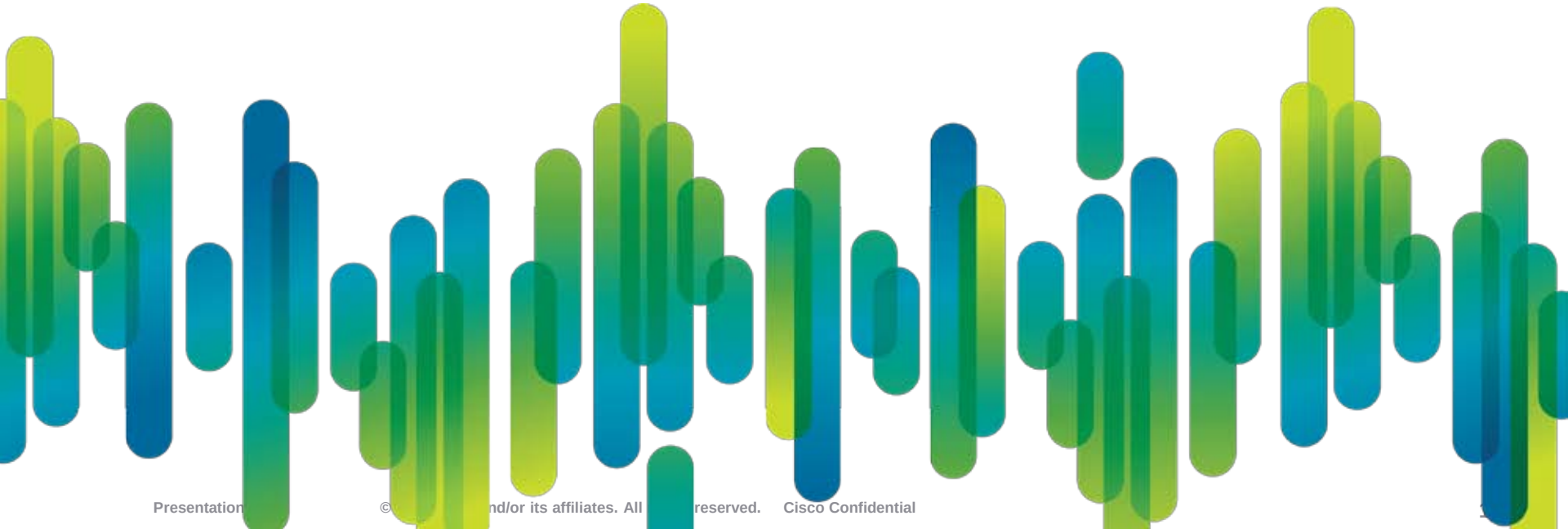
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The advantage of Gateway Cloning

1. Doors ➔ Templates ➔ Credential Templates - configure the credential format
2. Doors ➔ Templates ➔ Device Templates - assign the credential format to the appropriate reader type
3. Locations and Doors - Add base and location hierarchy
4. Doors ➔ Hardware - Use gateway template (say 2 reader template) to create gateway and doors.
5. Doors ➔ Access Policies - create access policies for the doors
6. Users ➔ Badges - add badges and assign to personnel. Also enable appropriate access policies (created in the last step) for these badges
7. Locations and Doors (or Hardware) ➔ Right click on Locations (or Gateway controller) and issue Apply Configuration Changes
8. Wait for gateway to connect and credential data to be sent to the gateway (takes a couple of minutes)
9. That's it
10. Now you can use **gateway cloning** to clone this gateway any number of times (only need to plug in the new gateway serial number and door names into the wizard)

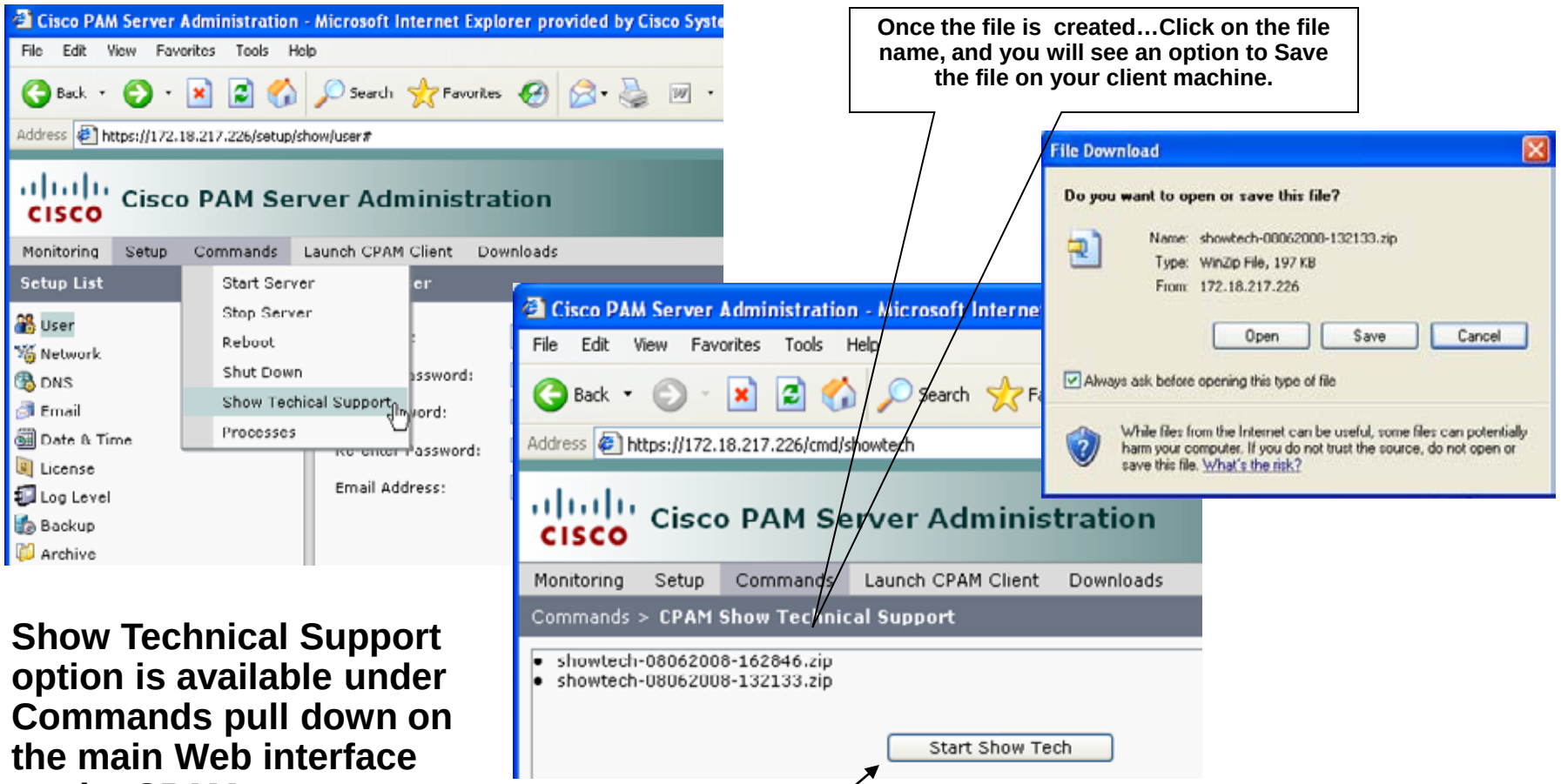
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting the system



© nd/or its affiliates. All reserved. Cisco Confidential

The infamous ‘show tech’ for CPAM


Cisco PAM Server Administration - Microsoft Internet Explorer provided by Cisco Syste
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.18.217.226/setup/show/user#
Cisco PAM Server Administration
Monitoring Setup Commands Launch CPAM Client Downloads
Setup List
User
Network
DNS
Email
Date & Time
License
Log Level
Backup
Archive
Start Server
Stop Server
Reboot
Shut Down
Show Technical Support
Processes
Email Address:
Cisco PAM Server Administration - Microsoft Interne
File Edit View Favorites Tools Help
Back Search
Address https://172.18.217.226/cmd/showtech
Cisco PAM Server Administration
Monitoring Setup Commands Launch CPAM Client Downloads
Commands > CPAM Show Technical Support
showtech-08062008-162846.zip
showtech-08062008-132133.zip
Start Show Tech
File Download
Do you want to open or save this file?
Name: showtech-08062008-132133.zip
Type: WinZip File, 197 KB
From: 172.18.217.226
Open Save Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Once the file is created…Click on the file name, and you will see an option to Save the file on your client machine.

Show Technical Support option is available under Commands pull down on the main Web interface on the CPAM server

Click on Start Show Tech

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

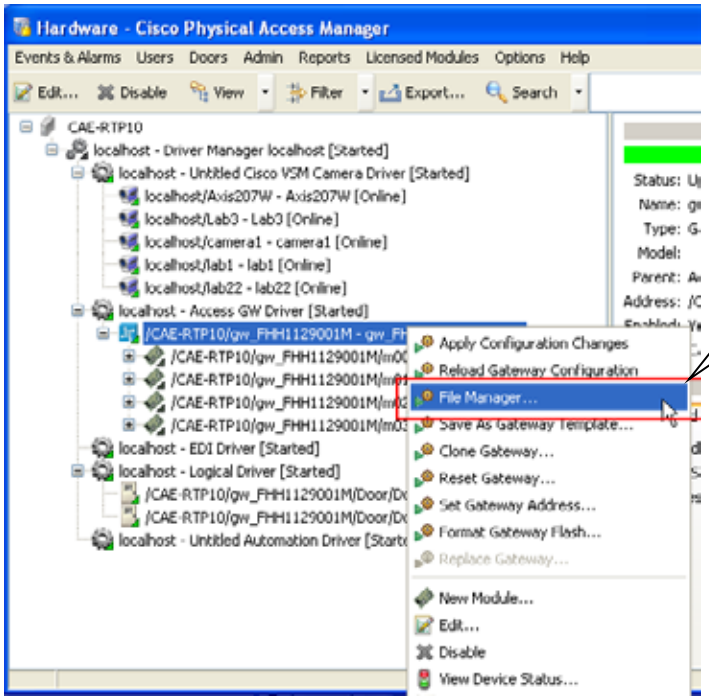
Gateway Log collection

- Performed via CPAM client using Gateway File Manager option.
- Once open, high light the file to upload, then click on Initiate Upload.
- When prompted, enter the IP address of the CPAM server. (you may have to include a / in the path field)
- Upload files as directed by support. Might want to upload all files as a precaution.
- Once files are uploaded to CPAM, we need to move them to the client machine, and email them to support.
- Create a folder on the client in C:\
- Upload log files from CPAM server to folder in C:\

In CPAM release 1.1 the Gateway ‘all logs file’ was introduced which will create a zip file containing all of the Gateway logs.

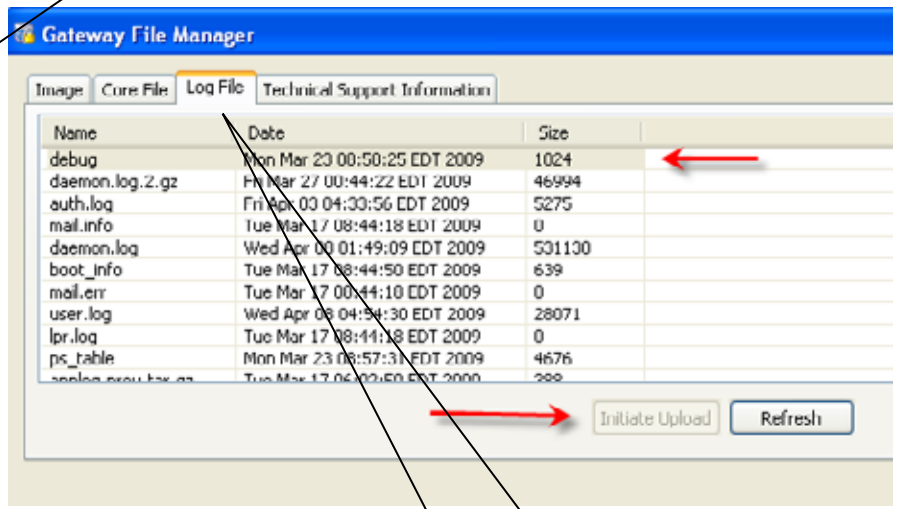
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Uploading logs to CPAM server



Left Click on the Gateway, then Right Click on File Manager to open the panel below

1

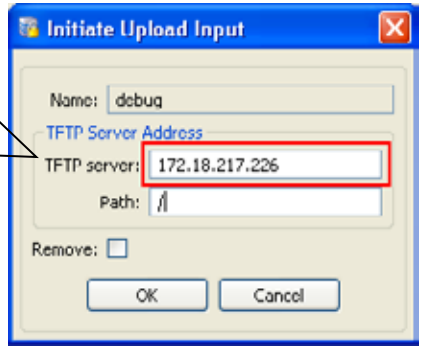


2

Once the panel is open, click on the Log File tab. Logs are uploaded 1 at a time. Click on the log file, then on Initiate Upload

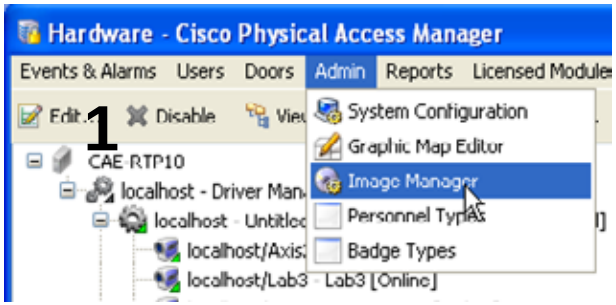
3

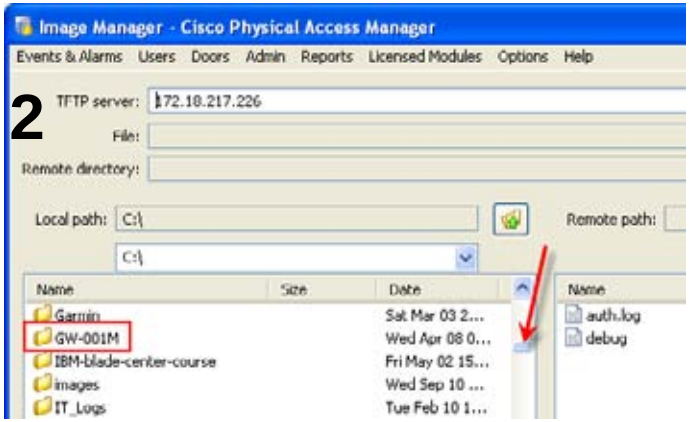
Enter the IP address of the CPAM server, and enter a / in the path. You can use a different TFTP server if one is available. Once the entries are completed, click OK to upload the file.



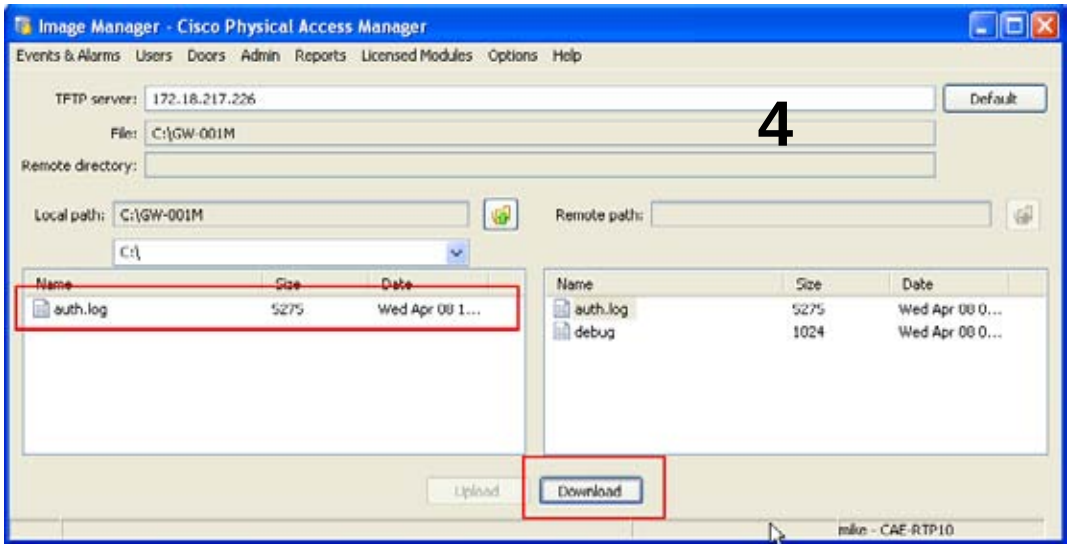
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

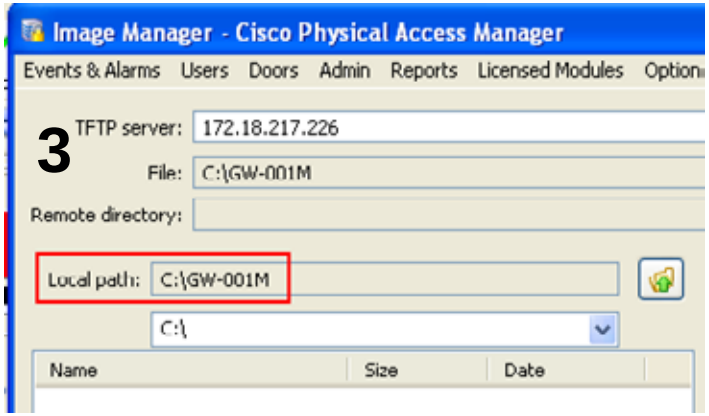
Moving file from the CPAM to client machine





Open Image Manager, then migrate to the folder in C:\ and double click the folder name. Once the Path is correct, click on the log file, and then click on Download.

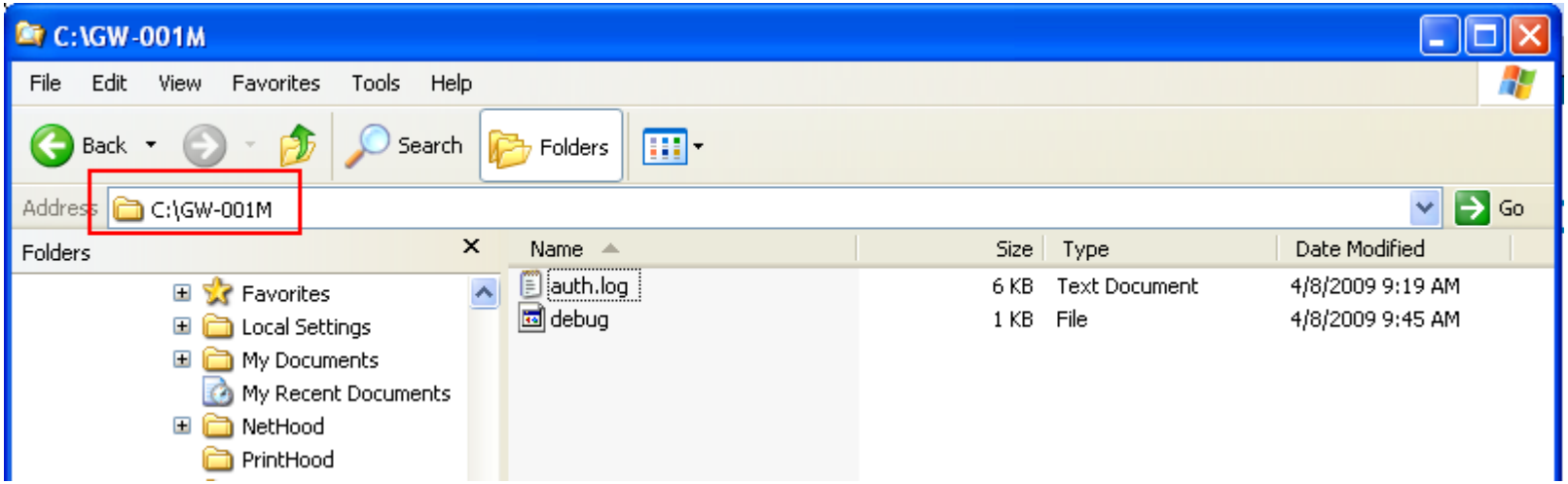




In this release we can not navigate the directories on the local machine. Only 1 file at a time may be downloaded.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zipping and emailing the Gateway Logs



Once the files are on the client machine, in the C:\ directory, they can be zipped into 1 file, and emailed to support.

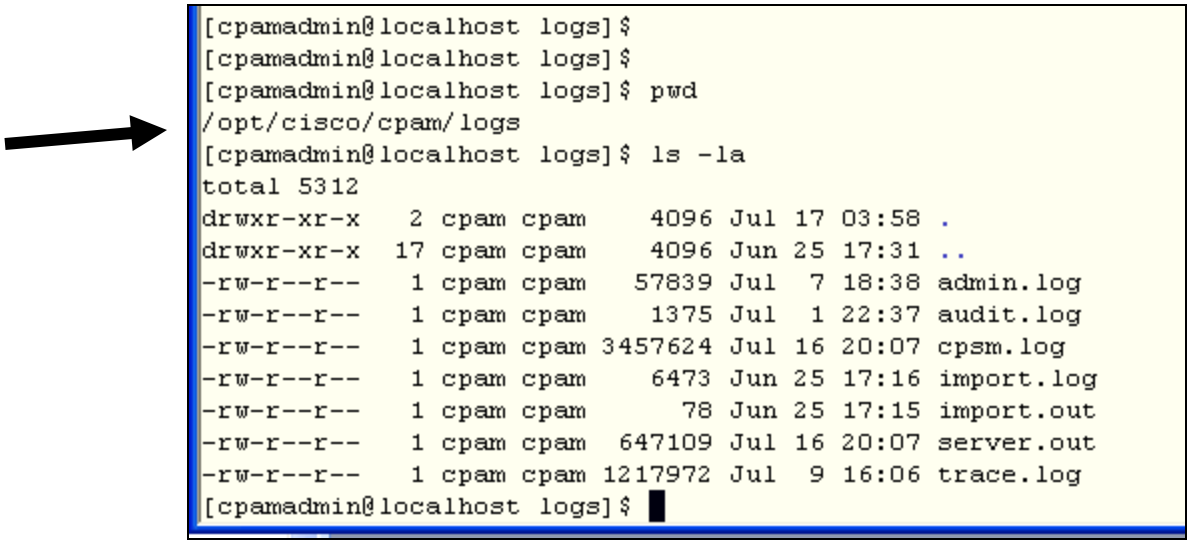
Best practice is to upload files one Gateway at a time, and use a different directory in C:\ for each Gateway. If the logs are zipped, create one zip file for each Gateway.

Good ideal would be to name the directory C:\GW-wxyx where wxyz are the last 4 characters of the Gateway serial number.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CPAM log collection

- SSH (user and password needed) into the CPAM server command line.
- Go to /opt/cisco/cpam/logs
- To view the logs use the ‘cat’ or ‘more’ command.



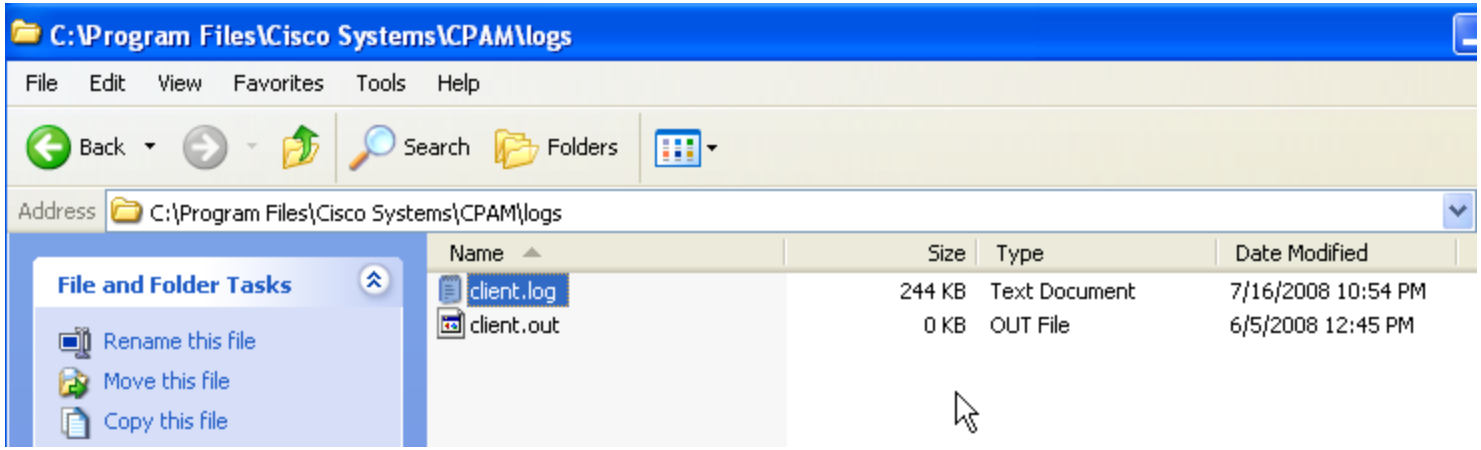
```
[cpamadmin@localhost logs]$
[cpamadmin@localhost logs]$
[cpamadmin@localhost logs]$ pwd
/opt/cisco/cpam/logs
[cpamadmin@localhost logs]$ ls -la
total 5312
drwxr-xr-x   2 cpam cpam    4096 Jul 17 03:58 .
drwxr-xr-x  17 cpam cpam    4096 Jun 25 17:31 ..
-rw-r--r--   1 cpam cpam   57839 Jul  7 18:38 admin.log
-rw-r--r--   1 cpam cpam    1375 Jul  1 22:37 audit.log
-rw-r--r--   1 cpam cpam 3457624 Jul 16 20:07 cpsm.log
-rw-r--r--   1 cpam cpam    6473 Jun 25 17:16 import.log
-rw-r--r--   1 cpam cpam      78 Jun 25 17:15 import.out
-rw-r--r--   1 cpam cpam  647109 Jul 16 20:07 server.out
-rw-r--r--   1 cpam cpam 1217972 Jul  9 16:06 trace.log
[cpamadmin@localhost logs]$
```

These files can be retrieved by SFTP from the CPAM server and zipped for emailing to the development engineers. The CPAM server is running an SFTP server, no configuration is necessary.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CPAM client logs

- Log is kept on the client machine where the client is running from.
- File can be zipped and emailed to development engineering as needed.


C:\Program Files\Cisco Systems\CPAM\logs
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\Cisco Systems\CPAM\logs
File and Folder Tasks
Rename this file
Move this file
Copy this file
Name Size Type Date Modified
client.log 244 KB Text Document 7/16/2008 10:54 PM
client.out 0 KB OUT File 6/5/2008 12:45 PM

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewall considerations

- TCP port 80 HTTP
- TCP port 443 HTTPS
- TCP port 1236 BVCONTROL
- TCP port 3306 MYSQL
- All these need to be open between the client machine and the CPAM server.

- Gateway to CPAM server uses TCP port 8020 by default.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Additional features

- Graphic Maps with active ICONs
- Quick Launch panels for 1 click action ICONs
- URL notifications sent upon trigger being met
- Integration with Active Directory for personnel import and login user authentication.
- Robust report generation
- Custom user roles to limit views and permissions

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential